

# ON THE EISENSTEIN IDEAL OF DRINFELD MODULAR CURVES

AMBRUS PÁL

April 14, 2006.

**ABSTRACT.** Let  $\mathfrak{E}(\mathfrak{p})$  denote the Eisenstein ideal in the Hecke algebra  $\mathbb{T}(\mathfrak{p})$  of the Drinfeld modular curve  $X_0(\mathfrak{p})$  parameterizing Drinfeld modules of rank two over  $\mathbb{F}_q[T]$  of general characteristic with Hecke level  $\mathfrak{p}$ -structure, where  $\mathfrak{p} \triangleleft \mathbb{F}_q[T]$  is a non-zero prime ideal. We prove that the characteristic  $p$  of the field  $\mathbb{F}_q$  does not divide the order of the quotient  $\mathbb{T}(\mathfrak{p})/\mathfrak{E}(\mathfrak{p})$  and the Eisenstein ideal  $\mathfrak{E}(\mathfrak{p})$  is locally principal.

## 1. INTRODUCTION

**Notation 1.1.** Let  $F = \mathbb{F}_q(T)$  denote the rational function field of transcendence degree one over a finite field  $\mathbb{F}_q$  of characteristic  $p$ , where  $T$  is an indeterminate, and let  $\mathbf{A} = \mathbb{F}_q[T]$ . Let  $Y_0(\mathfrak{n})$  be the Drinfeld modular curve parameterizing Drinfeld modules of rank two over  $\mathbb{F}_q[T]$  of general characteristic with Hecke level  $\mathfrak{n}$ -structure, where  $\mathfrak{n} \triangleleft \mathbb{F}_q[T]$  is a non-zero ideal. Let  $X_0(\mathfrak{n})$  denote the unique geometrically irreducible non-singular projective curve containing  $Y_0(\mathfrak{n})$  and let moreover  $J_0(\mathfrak{n})$  denote the Jacobian of the curve  $X_0(\mathfrak{n})$ . Assume now that  $\mathfrak{n} = \mathfrak{p}$  is a prime ideal and let  $\mathfrak{E}(\mathfrak{p})$  denote the Eisenstein ideal in the Hecke algebra  $\mathbb{T}(\mathfrak{p})$  of the Drinfeld modular curve  $X_0(\mathfrak{p})$ , defined in [22] first in this context. The latter was already studied intensively in [19] already. There a close analogue of the classical theory in [16] was worked out in detail. In this paper we will complete our previous results. In particular we show:

**Theorem 1.2.** *We have:*

$$\frac{\mathbb{T}(\mathfrak{p})}{\mathfrak{E}(\mathfrak{p})} = \frac{\mathbb{Z}}{N(\mathfrak{p})\mathbb{Z}},$$

where

$$N(\mathfrak{p}) = \begin{cases} \frac{q^{\deg(\mathfrak{p})}-1}{q-1}, & \text{if } \deg(\mathfrak{p}) \text{ is odd,} \\ \frac{q^{\deg(\mathfrak{p})}-1}{q^2-1}, & \text{otherwise.} \end{cases}$$

By the results of [19] the new information in the claim above is that the characteristic  $p$  does not divide the order  $|\mathbb{T}(\mathfrak{p})/\mathfrak{E}(\mathfrak{p})|$ . The latter has the following immediate

---

2000 *Mathematics Subject Classification.* 11G18 (primary), 11G09 (secondary).

**Corollary 1.3.** *There is no non-zero double-cuspidal, weight two Drinfeld modular form  $\phi \in M_{2,1}^2(\Gamma_0(\mathfrak{p}))$  of type 1 and level  $\mathfrak{p}$  fixed by the Hecke algebra  $\mathbb{T}(\mathfrak{p})$ .*

In fact we will prove a similar claim about  $M_{2,1}^2(\Gamma_0(\mathfrak{n}))$  for every square-free ideal  $\mathfrak{n} \triangleleft \mathbf{A}$ . The other main result of this paper is the following

**Theorem 1.4.** *The Eisenstein ideal  $\mathfrak{E}(\mathfrak{p})$  is locally principal.*

We are going to give two proofs of the result above. In the first proof theorem is deduced from the fact that the ring  $\mathbb{T}(\mathfrak{p})$  is locally Gorenstein at the prime ideals lying above the Eisenstein ideal, which we proved already in [19], by adopting Mazur's original argument to the modular symbols introduced in [23]. In fact we will produce explicit generators (for details see Theorem 4.17). In the second proof we will identify (a suitable enlargement of)  $\mathbb{T}(\mathfrak{p})$  with a universal deformation ring  $R(\mathfrak{p})$  analogous to the construction in [1] using the Wiles-Lenstra criterion, then prove that  $R(\mathfrak{p})$  is generated by one element over  $\mathbb{Z}_l$  using cohomological methods. The deformation theoretical methods prove directly the Gorenstein property without using much about the finer geometry of the modular curve  $X_0(\mathfrak{p})$  hence also give an alternative route to prove the main diophantine results of the paper [19].

**Contents 1.5.** In the next chapter we are going to prove that every abelian variety defined over  $F$  whose Néron model has either good ordinary reduction or multiplicative reduction at every closed point of the projective line over  $\mathbb{F}_q$  has everywhere good reduction. In the third chapter we prove some preliminary results about harmonic cochains. The result proved in the second chapter is used in the fourth chapter to prove Theorem 1.2 and Corollary 1.3 where we also define the Eisenstein ideal of the Jacobian of the Drinfeld modular curve  $X_0(\mathfrak{n})$ . In the fifth chapter we develop theory of modular symbols for Drinfeld modular curves, first studied by Teitelbaum in this context, and use it to give the first proof of Theorem 1.4. We introduce a deformation functor analogous to the one defined in [1] and prove that it is representable in the sixth chapter. In the seventh chapter we construct a homomorphism from the universal deformation ring of the functor introduced in the previous chapter into a certain Hecke algebra. We prove that this map is an isomorphism in the eighth chapter and deduce the second proof of Theorem 1.4 from this result. The aim of the ninth chapter is to deduce the main diophantine results of [19] directly from the Gorenstein property.

**Acknowledgment 1.6.** I wish to thank the IHÉS for its warm hospitality and the pleasant environment they created for productive research, where this article was written.

## 2. ABELIAN SCHEMES WITH MULTIPLICATIVE OR ORDINARY REDUCTION EVERYWHERE

**Definition 2.1.** Let  $\pi : A \rightarrow X$  be an abelian scheme of relative dimension  $d$  defined over an  $\mathbb{F}_p$ -scheme  $X$ , where  $p$  is a prime number. Let  $\pi^{(p^n)} : A^{(p^n)} \rightarrow X$  be the pull-back of  $A$  with respect to the  $n$ -iterated absolute Frobenius  $F^n : X \rightarrow X$  and let  $F^n : A \rightarrow A^{(p^n)}$  be the  $n$ -iterated relative Frobenius. Then  $A^{(p^n)}$  is an abelian scheme over  $X$  and  $F^n$  is a morphism of group schemes. We say that  $A$  is ordinary if the  $\mathbf{k}$ -valued points of  $A[p]$  form a group of order  $p^d$  for every geometric point  $\mathbf{k}$  of  $X$ . A finite flat group scheme  $G$  over  $X$  is called multiplicative if its Cartier dual is an étale group scheme.

**Proposition 2.2.** *Let  $A$  be an ordinary abelian scheme of dimension  $d$  over a noetherian  $\mathbb{F}_p$ -scheme  $X$ . Then  $F^n$  is flat, surjective and finite, and its kernel  $\text{Ker}(F^n)$  is a multiplicative finite flat group scheme of rank  $p^{nd}$  over  $X$ .*

**Proof.** This proposition is certainly well-known at least when  $X$  is the spectrum of a field. We deduce the general case from the above in the usual manner. The map  $F^n$  is flat because  $A$  is flat over  $X$  and  $F^n$  is flat on each fiber of  $A$  over  $X$  by Theorem 5.9 of section IV of [13], pages 99-100, known as the local criterion for flatness. The composition  $\pi = \pi^{(p^n)} \circ F^n$  and the map  $\pi^{(p^n)}$  are both proper and separated, hence  $F^n$  is proper, too. This map has finite fibers, so it is a finite map by Corollary 1.10 of [18], pages 6-7. As  $\text{Ker}(F^n)$  is the fiber of  $F^n$  over the zero section we get that it is finite and flat over  $X$ . On the other hand it is also a group scheme by definition. In order to prove the two remaining claims about the order and the multiplicativity of  $\text{Ker}(F^n)$ , it will be sufficient to show that the  $\mathbf{k}$ -valued points of the Cartier dual of  $\text{Ker}(F^n)$  form a group of order  $p^{nd}$  for every geometric point  $\mathbf{k}$  of  $X$  as the formation of the Cartier dual commutes with base change. The latter is just a reformulation of the claims mentioned above when  $X$  is the spectrum of an algebraically closed field.  $\square$

**Definition 2.3.** Let  $C$  denote a smooth irreducible curve defined over a field  $\mathbf{k}$  of characteristic  $p$ . For every closed point  $x$  of  $C$  let  $\mathcal{O}_x$  denote the local ring of  $C$  at  $x$ . Moreover let  $\widehat{\mathcal{O}}_x$ ,  $K_x$  denote the completion of  $\mathcal{O}_x$  and the quotient field of  $\widehat{\mathcal{O}}_x$ , respectively. Let  $K$  be the function field of  $C$  and let  $A$  be an abelian variety defined over  $K$ . Finally let  $\mathcal{A}$  denote the Néron model of  $A$  over  $C$ . Recall that  $A$  has multiplicative reduction at a closed point  $x$  if the connected component of the identity of the fiber of  $\mathcal{A}$  over  $x$  is a torus.

**Lemma 2.4.** *Assume that  $A$  has multiplicative reduction at the closed point  $x$  of  $C$ . Then  $\text{Ker}(F^n)$  in  $A$  extends to a multiplicative finite flat group scheme over  $\mathcal{O}_x$  of rank  $p^{nd}$ .*

**Proof.** It will be enough to show that the Cartier dual of  $\text{Ker}(F^n)$  extends to a finite étale group scheme over  $\mathcal{O}_x$ . In other words we need to show that the Galois representation attached to this étale group scheme is unramified. Since the formation of the Cartier dual commutes with base change, it will be enough to show that  $\text{Ker}(F^n)$  as a group scheme over  $\text{Spec}(K_x)$  extends to a multiplicative finite flat group scheme over  $\widehat{\mathcal{O}}_x$  of the prescribed rank. Since  $A$  has multiplicative reduction by assumption, it is semi-stable, and its Raynaud group, which is a smooth group scheme  $\mathcal{A}^\#$  over  $\widehat{\mathcal{O}}_x$  of finite type in general, is a torus. The formal completions of  $\mathcal{A}^\#$  and  $\mathcal{A}$  along the special fiber are equal. The finite flat group scheme  $\mathcal{A}^\#[p^n]$  is multiplicative of rank  $p^{nd}$  and annihilated by  $F^n$ , hence  $\mathcal{A}[p^n]$  also contains such a group scheme. The base change of the latter to  $\text{Spec}(K_x)$  lies in  $\text{Ker}(F^n)$ , but their rank is the same, so they must be equal.  $\square$

**Definition 2.5.** We will continue to use the notation above. For any category  $\mathcal{C}$  let  $\text{Ob}(\mathcal{C})$  denote the class of objects of  $\mathcal{C}$ . For any scheme  $X$  let  $\mathbf{FFGp}(X)$  denote the category of finite flat group schemes over  $X$ . For any morphism of schemes  $m : Y \rightarrow X$  let  $m^* : \mathbf{FFGp}(X) \rightarrow \mathbf{FFGp}(Y)$  denote the functor induced by the pull-back with respect to  $m$ . Let  $S$  be a finite set of closed points of  $C$  and let  $X$  denote the complement of  $S$  in  $C$ . Let  $j : \text{Spec}(F) \rightarrow X$  denote the generic point of  $X$  and let  $i : X \rightarrow C$  be its closed immersion into  $C$ . For every

$x$  closed point of  $C$  let  $j_x : \text{Spec}(F) \rightarrow \text{Spec}(\mathcal{O}_x)$  and  $i_x : \text{Spec}(\mathcal{O}_x) \rightarrow C$  be the generic point and closed immersion of the corresponding scheme, respectively. Let  $\mathbf{DD}(X, S)$  denote the additive category whose objects are collections of finite flat group schemes  $G_X \in \text{Ob}(\mathbf{FFGp}(X))$  and  $G_x \in \text{Ob}(\mathbf{FFGp}(\text{Spec}(\mathcal{O}_x)))$  for every  $x \in S$  and an isomorphism  $g_x : j_x^*(G_X) \rightarrow j_x^*(G_x)$  for every  $x \in S$ , and a morphism  $\phi : (G_X, G_x, g_x) \rightarrow (H_X, H_x, h_x)$  in this category is a collection of morphisms  $\phi_X : G_X \rightarrow H_X$  and  $\phi_x : G_x \rightarrow H_x$  for every  $x \in S$  such that  $j_x^*(\phi_x) \circ g_x = h_x \circ j_x^*(\phi_X)$ . Since  $j_x \circ i_x = j \circ i$  for every  $x$  closed point of  $C$ , there is a natural isomorphism  $c_x$  between the functors  $j_x^* \circ i_x^*$  and  $j^* \circ i^*$ . Let  $d$  denote the functor  $d : \mathbf{FFGp}(C) \rightarrow \mathbf{DD}(X, S)$  which assigns the object  $G \in \text{Ob}(\mathbf{FFGp}(C))$  the collection  $(i^*(G), i_x^*(G), c_x(G))$  and assigns the morphism  $\phi : G \rightarrow H$  the collection  $(i^*(\phi), i_x^*(\phi))$ . This is clearly a faithful embedding of categories.

**Lemma 2.6.** *The functor  $d$  is an equivalence of categories.*

**Proof.** The proof is an exercise in elementary descent theory. First we need to show that every object  $(G_X, G_x, g_x)$  of  $\mathbf{DD}(X, S)$  is in fact isomorphic to an object of  $\mathbf{FFGp}(C)$ . Since every finite and flat morphism is in fact affine, there is a coherent sheaf of Hopf algebras  $A_X$  over  $X$  and a coherent sheaf of Hopf algebras  $A_x$  over a Zariski neighborhood of  $x$  for every  $x \in S$  whose spectrum is  $G_X$  over  $X$  and  $G_x$  over  $\text{Spec}(\mathcal{O}_x)$ , respectively. These sheaves patch together to a coherent sheaf of Hopf algebras over  $C$  via the maps induced by the morphisms  $g_x$  whose spectrum is the finite flat group scheme  $G$  we were looking for. A similar argument shows that any morphism in  $\mathbf{DD}(X, S)$  comes from a morphism in  $\mathbf{FFGp}(C)$ .  $\square$

Now we assume that  $\mathbf{k}$  is a finite field and  $C$  is the projective line  $\mathbb{P}_{\mathbf{k}}^1$  over  $\mathbf{k}$ .

**Theorem 2.7.** *Let  $A$  be an abelian variety defined over  $K$  such that the Néron model  $\mathcal{A}$  of  $A$  has either good ordinary reduction or multiplicative reduction at every closed point of  $C$ . Then  $A$  has everywhere good reduction.*

**Proof.** We may assume that there is a degree one closed point  $c$  in  $C$  where  $A$  has good reduction by enlarging  $\mathbf{k}$  if necessary. Let  $\mathcal{B}$  denote the unique constant abelian group scheme over  $C$  whose fiber  $\mathcal{B}_c$  at  $c$  is isomorphic to the fiber  $\mathcal{A}_c$  of  $\mathcal{A}$  at  $c$ . Let  $S$  denote the set of closed points of  $C$  where  $A$  has multiplicative reduction and let  $X$  denote the complement of  $S$  in  $C$  as above. By Proposition 2.2 the kernel of  $F^n$  in the abelian scheme  $\mathcal{A}|_X$  is a multiplicative finite flat group scheme of rank  $p^{nd}$  over  $X$  where  $d$  is the dimension of  $A$  over  $K$ . On the other hand the kernel of  $F^n$  in the abelian variety  $A$  extends to a multiplicative finite flat group scheme over  $\mathcal{O}_x$  of rank  $p^{nd}$  for every  $x \in S$  by Lemma 2.4. These group schemes glue together to a finite flat group scheme  $A_n$  over  $C$  by Lemma 2.6. Since the property of being multiplicative is local with respect to the Zariski topology, this group scheme is multiplicative. Therefore its Cartier dual is étale. Since the geometric fundamental group of  $C$  is trivial, we get that  $A_n$  is the base change of a group scheme over  $\text{Spec}(\mathbf{k})$  with respect to the constant map  $C \rightarrow \text{Spec}(\mathbf{k})$ . Its fiber over  $c$  is isomorphic to the fiber of the kernel of  $F^n$  in  $\mathcal{B}|_X$  at  $c$ , so these group schemes must be isomorphic. Hence the fibers  $\mathcal{A}_x$  and  $\mathcal{B}_x$  must be isogenous for every closed point  $x$  in  $X$  by Lemma 2.8 below. Therefore  $A$  and  $B$  must be isogenous by Zarhin's isogeny theorem where  $B$  is the generic fiber of  $\mathcal{B}$ . In particular  $A$  has everywhere good reduction.  $\square$

**Lemma 2.8.** *Let  $\mathbf{f}$  be a finite field of characteristic  $p$  and let  $C_1$  and  $C_2$  be two ordinary abelian varieties of same dimension defined over  $\mathbf{f}$ . Assume that the kernel of  $F^n$  in  $C_1$  and in  $C_2$  are isomorphic as group schemes for every positive integer  $n$ . Then  $C_1$  and  $C_2$  are isogenous over  $\mathbf{f}$ .*

**Proof.** Let  $\mathbb{W}(\mathbf{f})$  and  $\mathbb{Q}(\mathbf{f})$  denote the Witt vectors of infinite length over  $\mathbf{f}$  and its quotient field, respectively. Let  $\sigma : \mathbb{Q}(\mathbf{f}) \rightarrow \mathbb{Q}(\mathbf{f})$  denote the Frobenius. For any finite flat group scheme  $G$  over  $\mathbf{f}$  let  $\mathbb{D}(G)$  denote its contravariant Dieudonné module. Because  $C_1$  and  $C_2$  are ordinary, there are exact sequences:

$$0 \rightarrow M_{i,n} \rightarrow C_i[p^n] \rightarrow N_{i,n} \rightarrow 0,$$

where  $M_{i,n}$ ,  $N_{i,n}$  are multiplicative and étale group schemes of rank  $p^{nd}$ , respectively, for  $i = 1$  or  $i = 2$  and every  $n \in \mathbb{N}$ . Recall that the Dieudonné crystal  $\mathbb{D}(V)$  associated to an abelian variety  $V$  over  $\mathbf{f}$  is defined as the limit of the Dieudonné modules  $\mathbb{D}(V[p^n])$  with respect to the maps  $\mathbb{D}(V[p^m]) \rightarrow \mathbb{D}(V[p^n])$  induced by the closed immersions  $V[p^n] \rightarrow V[p^m]$  for every  $n \leq m$ . By our assumption the group schemes  $M_{1,n}$  and  $M_{2,n}$  are isomorphic for every  $n \in \mathbb{N}$ . Because there are only finitely many isomorphisms between  $M_{1,n}$  and  $M_{2,n}$ , we may choose one  $\phi_n : M_{1,n} \rightarrow M_{2,n}$  for every  $n$  such that  $\phi_n|_{M_{1,m}} = \phi_m$  for every  $m \leq n$  by Tychonov's theorem. Hence the exact sequence above induces an exact sequence:

$$0 \rightarrow \mathbb{N}_i \rightarrow \mathbb{D}(C_i) \rightarrow \mathbb{M} \rightarrow 0$$

for  $i = 1$  or  $i = 2$ , where  $\mathbb{M}$  is a Dieudonné crystal of slope 1 and  $\mathbb{N}_i$  are Dieudonné crystals of slope 0. Recall that for every  $F$ -crystal  $\mathbb{V} = (V, \phi)$  over  $\mathbb{Q}(\mathbf{f})$ , where  $V$  is a finite dimensional vector space over  $\mathbb{Q}(\mathbf{f})$  and  $\phi : V \rightarrow V$  is a bijective  $\sigma$ -linear map, its dual  $\mathbb{V}^\vee$  is defined as the pair  $(\text{Hom}_{\mathbb{Q}(\mathbf{f})}(V, \mathbb{Q}(\mathbf{f})), \phi^\vee)$ , where  $\phi^\vee(f)(u) = pf(\phi^{-1}(u))^\sigma$  for every  $f \in \text{Hom}_{\mathbb{Q}(\mathbf{f})}(V, \mathbb{Q}(\mathbf{f}))$  and  $u \in V$ . Every choice of polarization of  $C_i$  induces an isomorphism of  $F$ -crystals  $(\mathbb{D}(C_i) \otimes_{\mathbb{W}(\mathbf{f})} \mathbb{Q}(\mathbf{f}))^\vee = \mathbb{D}(C_i) \otimes_{\mathbb{W}(\mathbf{f})} \mathbb{Q}(\mathbf{f})$  over  $\mathbb{Q}(\mathbf{f})$ . Such an isomorphism induces an isomorphism between the largest quotient modules of slope 1 which are equal to  $(\mathbb{M} \otimes_{\mathbb{W}(\mathbf{f})} \mathbb{Q}(\mathbf{f}))^\vee$  and  $\mathbb{N}_i \otimes_{\mathbb{W}(\mathbf{f})} \mathbb{Q}(\mathbf{f})$ , respectively. Therefore the semi-simplifications of  $\mathbb{D}(C_i) \otimes_{\mathbb{W}(\mathbf{f})} \mathbb{Q}(\mathbf{f})$ , where  $i = 1$  or  $i = 2$ , are isomorphic. Hence the characteristic polynomial of the arithmetic Frobenius of the Dieudonné crystals  $\mathbb{D}(C_1)$  and  $\mathbb{D}(C_2)$  are equal which implies that  $C_1$  and  $C_2$  must be isogenous by Honda-Tate theory.  $\square$

### 3. HARMONIC COCHAINS

**Definition 3.1.** For any graph  $G$  let  $\mathcal{V}(G)$  and  $\mathcal{E}(G)$  denote its set of vertices and edges, respectively. In this paper we will only consider such oriented graphs  $G$  which are equipped with an involution  $\bar{\cdot} : \mathcal{E}(G) \rightarrow \mathcal{E}(G)$  such that for each edge  $e \in \mathcal{E}(G)$  the original and terminal vertices of the edge  $\bar{e} \in \mathcal{E}(G)$  are the terminal and original vertices of  $e$ , respectively. The edge  $\bar{e}$  is called the edge  $e$  with reversed orientation. Let  $R$  be a commutative group. A function  $\phi : \mathcal{E}(G) \rightarrow R$  is called a harmonic  $R$ -valued cochain, if it satisfies the following conditions:

(i) We have:

$$\phi(e) + \phi(\bar{e}) = 0 \quad (\forall e \in \mathcal{E}(G)).$$

- (ii) If for an edge  $e$  we introduce the notation  $o(e)$  and  $t(e)$  for its original and terminal vertex respectively,

$$\sum_{\substack{e \in \mathcal{E}(G) \\ o(e)=v}} \phi(e) = 0 \quad (\forall v \in \mathcal{V}(G)).$$

We denote by  $H(G, R)$  the group of  $R$ -valued harmonic cochains on  $G$ .

**Definition 3.2.** Let  $GL_2$  denote the group scheme of invertible two by two matrices and let  $Z$  denote its center. Let  $F_\infty$  denote the completion of  $F = \mathbb{F}_q(T)$  with respect to the valuation  $\infty$  corresponding to the point at infinity on the projective line over  $\mathbb{F}_q$ . Let  $\mathcal{O}_\infty$  denote the valuation ring of  $F_\infty$  and let  $v \in F_\infty$  be a uniformizer. We are going to recall the definition of the Bruhat-Tits tree  $\mathcal{T}$  associated to the projective linear group  $PGL_2(F_\infty)$ . The set of vertices  $\mathcal{V}(\mathcal{T})$  and edges  $\mathcal{E}(\mathcal{T})$  are the cosets  $GL_2(F_\infty)/GL_2(\mathcal{O}_\infty)Z(F_\infty)$  and  $GL_2(F_\infty)/\Gamma_\infty Z(F_\infty)$ , respectively, where  $\Gamma_\infty$  is the Iwahori group:

$$\Gamma_\infty = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O}_\infty) \mid \infty(c) > 0 \right\}.$$

Since  $\Gamma_\infty$  is a subgroup of  $GL_2(\mathcal{O}_\infty)$  there is a natural morphism  $o : \mathcal{E}(\mathcal{T}) \rightarrow \mathcal{V}(\mathcal{T})$  which assigns to every edge its original vertex. The matrix  $\begin{pmatrix} 0 & 1 \\ v & 0 \end{pmatrix}$  normalizes the Iwahori subgroup therefore the map  $GL_2(F_\infty) \rightarrow GL_2(F_\infty)$  given by the rule  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ v & 0 \end{pmatrix}$  induces a map on the coset  $\mathcal{V}(\mathcal{T})$ . This map is the involution which assigns to every edge  $e$  the same edge  $\bar{e}$  with reversed orientation. The composition of this involution and the map  $o$  is the map  $t : \mathcal{E}(\mathcal{T}) \rightarrow \mathcal{V}(\mathcal{T})$  which assigns to every edge its terminal vertex.

**Definition 3.3.** For every non-zero ideal  $\mathfrak{n} \triangleleft \mathbf{A}$  let  $\Gamma_0(\mathfrak{n})$  denote the Hecke congruence group:

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{A}) \mid c \equiv 0 \pmod{\mathfrak{n}} \right\}.$$

The group  $GL_2(F_\infty)$  acts on itself via its left-regular action which induces an action of  $GL_2(F_\infty)$  on the Bruhat-Tits tree. This action induces an action of its subgroup  $\Gamma_0(\mathfrak{n})$  on  $\mathcal{T}$  as well. Let  $H(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$  denote the group of  $\Gamma_0(\mathfrak{n})$ -invariant  $R$ -valued cochains on  $\mathcal{T}$ . The group  $GL_2(\mathbf{A})$  does not contain elements which map an edge  $e \in \mathcal{E}(\mathcal{T})$  to the same edge  $\bar{e}$  with reversed orientation therefore the cosets  $\Gamma_0(\mathfrak{n}) \backslash \mathcal{V}(\mathcal{T})$  and  $\Gamma_0(\mathfrak{n}) \backslash \mathcal{E}(\mathcal{T})$  are the vertices and edges of an oriented graph which is going to be denoted by  $\Gamma_0(\mathfrak{n}) \backslash \mathcal{T}$ . Every element  $\phi$  of  $H(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$  induces an  $R$ -valued function on the edges of  $\Gamma_0(\mathfrak{n}) \backslash \mathcal{T}$ . If this function is zero outside of a finite set we say that  $\phi$  is cuspidal. The  $R$ -module of cuspidal elements of  $H(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$  is denoted by  $H_!(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$ . Finally let  $H_{!!}(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$  denote the image of the canonical map  $H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{n})} \otimes R \rightarrow H_!(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$ .

**Definition 3.4.** For every pair  $\mathfrak{m}, \mathfrak{n} \triangleleft \mathbf{A}$  of non-zero ideals let  $H(\mathfrak{m}, \mathfrak{n})$  denote the set:

$$H(\mathfrak{m}, \mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(F) \mid a, b, c, d \in \mathbf{A}, (ad - cb) = \mathfrak{m}, \mathfrak{n} \supseteq (c), (d) + \mathfrak{n} = \mathbf{A} \right\}.$$

The set  $H(\mathfrak{m}, \mathfrak{n})$  is finite and it is a double  $\Gamma_0(\mathfrak{n})$ -coset, so it is a disjoint union of finitely many left  $\Gamma_0(\mathfrak{n})$ -cosets. Let  $R(\mathfrak{m}, \mathfrak{n})$  be a set of representatives of these cosets. For any left  $\Gamma_0(\mathfrak{n})$ -invariant  $R$ -valued function  $\phi : \mathcal{E}(\mathcal{T}) \rightarrow R$  define  $T_{\mathfrak{m}}(\phi)$  by the formula:

$$T_{\mathfrak{m}}(\phi)(g) = \sum_{h \in R(\mathfrak{m}, \mathfrak{n})} \phi(hg), \quad \forall g \in \mathcal{E}(\mathcal{T}).$$

It is well-known and easy to check that  $T_{\mathfrak{m}}(\phi)$  is independent of the choice of  $R(\mathfrak{m}, \mathfrak{n})$  and it is also a left  $\Gamma_0(\mathfrak{n})$ -invariant  $R$ -valued function so we have an  $R$ -linear operator  $T_{\mathfrak{m}}$  acting on the  $R$ -module of left  $\Gamma_0(\mathfrak{n})$ -invariant  $R$ -valued functions on  $\mathcal{E}(\mathcal{T})$ . It is also well-known and not too difficult to verify that  $T_{\mathfrak{m}}$  leaves the submodules  $H(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$  and  $H_1(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$  invariant.

**Notation 3.5.** Let  $\Omega$  denote the rigid analytic upper half plane, or Drinfeld's upper half plane over  $F_{\infty}$ . The set of points of  $\Omega$  is  $\mathbb{C}_{\infty} - F_{\infty}$ , denoted also by  $\Omega$  by abuse of notation, where  $\mathbb{C}_{\infty}$  is the completion of the algebraic closure of  $F_{\infty}$ . For the definition of its rigid analytic structure as well as the other concepts recalled below see for example [12]. For each holomorphic function  $u : \Omega \rightarrow \mathbb{C}_{\infty}^*$  let  $r(u) : \mathcal{E}(\mathcal{T}) \rightarrow \mathbb{Z}$  denote the van der Put logarithmic derivative of  $u$  (see [12], page 40). The group  $GL_2(\mathbf{A})$  acts on Drinfeld's upper half plane  $\Omega$  on the left via Möbius transformations. This action is discrete hence the set  $\Gamma_0(\mathfrak{n}) \backslash \Omega$  is equipped naturally with the structure of a rigid analytic curve. Let  $Y_0(\mathfrak{n})$  also denote the underlying rigid analytical space of the base change of  $Y_0(\mathfrak{n})$  to  $F_{\infty}$  by abuse of notation.

**Theorem 3.6.** *There is a rigid-analytical isomorphism:*

$$Y_0(\mathfrak{n}) \cong \Gamma_0(\mathfrak{n}) \backslash \Omega.$$

**Proof.** This is a special case of Theorem 6.6 of [4].  $\square$

**Notation 3.7.** If  $\psi : \mathbf{A} \rightarrow \mathbb{C}_{\infty} \{ \tau \}$  is a Drinfeld module of rank two over  $\mathbf{A}$ , then

$$\psi(T) = T + g(\psi)\tau + \Delta(\psi)\tau^2,$$

where  $\Delta$  is the Drinfeld discriminant function. It is a Drinfeld modular form of weight  $q^2 - 1$ . Under the identification of Theorem 3.5 the Drinfeld discriminant function  $\Delta$  is a nowhere vanishing holomorphic function on  $\Omega$ . For every ideal  $\mathfrak{n} = (n) \triangleleft \mathbf{A}$  let  $\Delta_{\mathfrak{n}}$  denote the modular form of weight  $q^2 - 1$  given by the formula  $\Delta_{\mathfrak{n}}(z) = \Delta(nz)$ . As the notation indicates  $\Delta_{\mathfrak{n}}$  is independent of the choice of the generator  $n \in \mathfrak{n}$ . Let  $E_{\mathfrak{n}} = r(\Delta/\Delta_{\mathfrak{n}})$ . Since  $\Delta/\Delta_{\mathfrak{n}}$  is a modular form of weight zero, i.e. it is a modular unit, the function  $E_{\mathfrak{n}}$  is a  $\mathbb{Z}$ -valued harmonic cochain invariant under the action of  $\Gamma_0(\mathfrak{n})$  because the van der Put derivative is equivariant with respect to the action of  $GL_2(\mathbf{A})$ . For the rest of this chapter assume that  $\mathfrak{n} = \mathfrak{p}$  is a proper prime ideal. Let  $\pi \in \mathbf{A}$  be the unique monic polynomial generating  $\mathfrak{p}$ . For every left  $\Gamma_0(\mathfrak{p})$ -invariant  $R$ -valued function  $\phi : \mathcal{E}(\mathcal{T}) \rightarrow R$  define  $W_{\mathfrak{p}}(\phi)$  by the formula:

$$W_{\mathfrak{p}}(\phi)(g) = \phi\left(\begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix} g\right), \quad \forall g \in \mathcal{E}(\mathcal{T}).$$

Because the matrix in the formula above normalizes  $\Gamma_0(\mathfrak{p})$  the function  $W_{\mathfrak{p}}(\phi)$  is also left  $\Gamma_0(\mathfrak{p})$ -invariant.

**Lemma 3.8.** *We have:*

$$W_{\mathfrak{p}}(E_{\mathfrak{p}}) = -E_{\mathfrak{p}} \text{ and } T_{\mathfrak{q}}(E_{\mathfrak{p}}) = (1 + q^{\deg(\mathfrak{q})})E_{\mathfrak{p}}$$

for every prime ideal  $\mathfrak{q} \triangleleft \mathbf{A}$  different from  $\mathfrak{p}$ .

**Proof.** This is Lemma 6.2 of [19] on page 153-154.  $\square$

**Definition 3.9.** Let  $\mu_{\infty}$  be a Haar measure on the additive group of  $F_{\infty}$  and for every  $g \in GL_2(F_{\infty})$  let the same symbol denote the edge of  $\mathcal{T}$  corresponding to the coset of  $g$  in  $GL_2(F_{\infty})/\Gamma_{\infty}Z(F_{\infty})$ . For every left  $\Gamma_0(\mathfrak{p})$ -invariant complex-valued function  $\phi$  on  $\mathcal{E}(\mathcal{T})$  the integral

$$\phi^0 = \int_{\mathbf{A} \setminus F_{\infty}} \phi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right) d\mu_{\infty}(x)$$

is well-defined as the integrand is invariant under translation by elements of  $\mathbf{A}$  and the domain of integration is compact.

**Proposition 3.10.** *A harmonic cochain  $\phi \in H(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})}$  is cuspidal if and only if the integrals  $\phi^0$  and  $W_{\mathfrak{p}}(\phi)^0$  are both zero.*

**Proof.** This is Proposition 6.3 of [19] on page 154-155.  $\square$

We will also need the following

**Lemma 3.11.** *The group  $H(\mathcal{T}, \mathbb{C})^{GL_2(\mathbf{A})}$  is trivial.*

**Proof.** Follows from Proposition 3.8 of [19] on pages 140-141.  $\square$

**Theorem 3.12.** *We have:*

$$H(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})} = H_1(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})} \bigoplus \mathbb{C}E_{\mathfrak{p}}.$$

**Proof.** According to Proposition 5.8 of [19] on pages 151-152 the integral  $E_{\mathfrak{p}}^0$  is not zero hence  $E_{\mathfrak{p}}$  is not an element of  $H_1(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})}$  by Proposition 3.10 above. On the other hand  $E_{\mathfrak{p}}^0 = -W_{\mathfrak{p}}(E_{\mathfrak{p}})^0$  by Lemma 3.8. Hence it will be sufficient to prove that the same identity holds for every harmonic cochain  $\phi \in H(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})}$  by Proposition 3.10. Let  $R(\mathfrak{p}) \subset \mathbb{F}_q[T]$  denote the set of polynomials whose degree is less than  $\deg(\mathfrak{p})$  and let  $S(\mathfrak{p})$  denote the set

$$S(\mathfrak{p}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & 1 \\ 1 & r \end{pmatrix} \mid r \in R(\mathfrak{p}) \right\}.$$

Then  $S(\mathfrak{p})$  is a set of representatives of the left  $\Gamma_0(\mathfrak{p})$ -cosets of  $GL_2(\mathbf{A})$  hence the function:

$$g \mapsto \sum_{s \in S(\mathfrak{p})} \phi(sg), \quad \forall g \in \mathcal{E}(\mathcal{T})$$

is an element of  $H(\mathcal{T}, \mathbb{C})^{GL_2(\mathbf{A})}$ . Therefore this function is zero by Lemma 3.11. In particular the integral:

$$\begin{aligned} \int_{\mathbf{A} \setminus F_{\infty}} \sum_{s \in S(\mathfrak{p})} \phi\left(s \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right) d\mu_{\infty}(x) &= \phi^0 + \int_{\mathbf{A} \setminus F_{\infty}} \sum_{r \in R(\mathfrak{p})} W_{\mathfrak{p}}(\phi)\left(\begin{pmatrix} \frac{1}{\pi} & \frac{x+r}{\pi} \\ 0 & 1 \end{pmatrix}\right) d\mu_{\infty}(x) \\ &= \phi^0 + \int_{\pi\mathbf{A} \setminus F_{\infty}} W_{\mathfrak{p}}(\phi)\left(\begin{pmatrix} \frac{1}{\pi} & \frac{x}{\pi} \\ 0 & 1 \end{pmatrix}\right) d\mu_{\infty}(x) \end{aligned}$$



is zero. Since  $W_{\mathfrak{p}}(\phi)$  is a harmonic cochain, it satisfies the identity:

$$W_{\mathfrak{p}}(\phi)(g) = \sum_{\epsilon \in \mathbb{F}_q} W_{\mathfrak{p}}(\phi)\left(g \begin{pmatrix} v & \epsilon \\ 0 & 1 \end{pmatrix}\right), \quad \forall g \in GL_2(F_{\infty})$$

where  $v \in F_{\infty}$  is a uniformizer. By a  $\deg(\mathfrak{p})$ -fold application of this identity we get the formula:

$$\begin{aligned} W_{\mathfrak{p}}(\phi)^0 &= \int_{A \setminus F_{\infty}} \sum_{\epsilon \in \mathbb{F}_q} W_{\mathfrak{p}}(\phi) \begin{pmatrix} v & x + \epsilon \\ 0 & 1 \end{pmatrix} d\mu_{\infty}(x) \\ &= \int_{v^{-1}A \setminus F_{\infty}} W_{\mathfrak{p}}(\phi) \begin{pmatrix} v & vx \\ 0 & 1 \end{pmatrix} d\mu_{\infty}(x) \\ &= \dots = \int_{\pi A \setminus F_{\infty}} W_{\mathfrak{p}}(\phi) \begin{pmatrix} \frac{1}{\pi} & \frac{x}{\pi} \\ 0 & 1 \end{pmatrix} d\mu_{\infty}(x). \end{aligned}$$

The claim is now clear.  $\square$

**Corollary 3.13.** *The  $\mathbb{Z}$ -module  $H(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$  is finitely generated and free.*

**Proof.** We are going to show that for every  $\mathbb{C}$ -subspace  $W$  of finite dimension  $n$  of the space of  $\mathbb{C}$ -valued functions on a set  $X$  there is a subset  $S \subset X$  of cardinality  $n$  such that every element of  $W$  is uniquely determined by its restriction to  $S$ . This claim clearly implies the proposition above by Theorem 3.12 as the vector space  $H_1(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{p})}$  is finite dimensional by a classical theorem of Harder. When  $n = 0$  the claim is obvious. Assume now that it is true for  $n - 1$  and pick a point  $x \in X$  such that not every element of  $W$  is zero at  $x$ . Then the  $\mathbb{C}$ -subspace  $V$  of elements of  $W$  vanishing at  $x$  has dimension  $n - 1$  hence there is a set  $R \subset X - \{x\}$  such that every element of  $V$  is uniquely determined by its restriction to  $R$ . The set  $S = R \cup \{x\}$  clearly satisfies the required property.  $\square$

#### 4. DRINFELD MODULAR FORMS AND QUOTIENTS OF THE MODULAR JACOBIAN

**Definition 4.1.** For every proper ideal  $\mathfrak{m} \triangleleft \mathbf{A}$  there is a  $\mathfrak{m}$ -th Hecke correspondence on the Drinfeld modular curve  $X_0(\mathfrak{n})$  which in turn induces an endomorphism of the Jacobian  $J_0(\mathfrak{n})$  of the curve, called the Hecke operator  $T_{\mathfrak{m}}$  (for a detailed description see for example [6] or [7].) The operator  $T_{\mathfrak{m}}$  is denoted by the same symbol we use for the operators introduced in Definition 3.4, but this will not cause confusion as we will see. For the moment it is sufficient to remark that they act on different objects. Let  $\mathbb{T}'(\mathfrak{n})$  denote the algebra with unity generated by the endomorphisms  $T_{\mathfrak{q}}$  of the Jacobian  $J_0(\mathfrak{n})$ , where  $\mathfrak{q} \triangleleft \mathbf{A}$  is any prime ideal which does not divide  $\mathfrak{n}$ . Let  $J_0^{old}(\mathfrak{n})$  be the smallest abelian sub-variety of  $J_0(\mathfrak{n})$  which is left invariant under the action of  $\mathbb{T}'(\mathfrak{n})$  and contains the image of  $J_0(\mathfrak{m})$  with respect to the map  $J_0(\mathfrak{m}) \rightarrow J_0(\mathfrak{n})$  induced by the degeneracy map  $X_0(\mathfrak{n}) \rightarrow X_0(\mathfrak{m})$  via Picard functoriality for every ideal  $\mathfrak{m} \supsetneq \mathfrak{n}$  of  $\mathbf{A}$ . Let  $J_0^{new}(\mathfrak{n})$  denote the quotient of  $J_0(\mathfrak{n})$  by  $J_0^{old}(\mathfrak{n})$ . The abelian variety  $J_0^{new}(\mathfrak{n})$  is naturally equipped with an action of  $\mathbb{T}'(\mathfrak{n})$  which makes the quotient map  $J_0(\mathfrak{n}) \rightarrow J_0^{new}(\mathfrak{n})$  a  $\mathbb{T}'(\mathfrak{n})$ -equivariant homomorphism. Let  $\mathbb{T}(\mathfrak{n})$  denote the image of  $\mathbb{T}'(\mathfrak{n})$  in  $\text{End}_F(J_0^{new}(\mathfrak{n}))$  corresponding to this action and let  $T_{\mathfrak{q}}$  denote the image of the Hecke operator  $T_{\mathfrak{q}}$  under the quotient map  $\mathbb{T}'(\mathfrak{n}) \rightarrow \mathbb{T}(\mathfrak{n})$  for every prime ideal  $\mathfrak{q} \triangleleft \mathbf{A}$  which does not divide  $\mathfrak{n}$  by the usual abuse of notation.

The algebra  $\mathbb{T}(\mathfrak{n})$  is known to be commutative. Let  $\mathfrak{E}(\mathfrak{n})$  denote the ideal of  $\mathbb{T}(\mathfrak{n})$  generated by the elements  $T_{\mathfrak{q}} - q^{\deg(\mathfrak{q})} - 1$ , where  $\mathfrak{q} \nmid \mathfrak{n}$  is any prime. The algebra  $\mathbb{T}(\mathfrak{n})$  will be called the Hecke algebra and  $\mathfrak{E}(\mathfrak{n})$  is its Eisenstein ideal, although these differ slightly from the usual definition, since they do not involve the Atkin-Lehmer operator. The latter will play no role in what follows. By Lemma 4.2 below the  $\mathbb{T}(\mathfrak{n})/\mathfrak{E}(\mathfrak{n})$  quotient is finite: we say that a prime number  $l$  is an Eisenstein prime for  $\mathfrak{n}$  if  $l$  divides  $|\mathbb{T}(\mathfrak{n})/\mathfrak{E}(\mathfrak{n})|$ . Note that  $J_0^{old}(\mathfrak{n})$  is a point when  $\mathfrak{n}$  is a proper prime ideal as  $X_0(1)$  is a rational curve. In particular our definition agrees with the one introduced in Definition 7.10 of [19] on page 160 in this particular case.

**Lemma 4.2.** *The quotient  $\mathbb{T}(\mathfrak{n})/\mathfrak{E}(\mathfrak{n})$  is finite and the natural injection  $\mathbb{Z} \rightarrow \mathbb{T}(\mathfrak{n})$  induces a surjective homomorphism  $\mathbb{Z} \rightarrow \mathbb{T}(\mathfrak{n})/\mathfrak{E}(\mathfrak{n})$ .*

**Proof.** It is clear from the definition that every generator  $T_{\mathfrak{q}}$  of  $\mathbb{T}(\mathfrak{n})$  is congruent to an element of  $\mathbb{Z}$  modulo the Eisenstein ideal, so the natural inclusion of  $\mathbb{Z}$  in  $\mathbb{T}(\mathfrak{n})$  induces a surjection  $\mathbb{Z} \rightarrow \mathbb{T}(\mathfrak{n})/\mathfrak{E}(\mathfrak{n})$ . If the quotient  $\mathbb{T}(\mathfrak{n})/\mathfrak{E}(\mathfrak{n})$  is not finite then this map is also injective, hence the Eisenstein ideal generates a non-trivial ideal in  $\mathbb{T}(\mathfrak{n}) \otimes_{\mathbb{Z}} \mathbb{Q}$ . Fix a prime  $l$  different from the characteristic  $p$ . Let  $\overline{F}$  denote the separable closure of  $F$  and let  $J_0(\mathfrak{n})_{\overline{F}}$  denote the base change of  $J_0(\mathfrak{n})$  to the spectrum of  $\overline{F}$ . The action of  $\mathbb{T}'(\mathfrak{n})$  on  $J_0(\mathfrak{n})$  induces an action on the étale cohomology group  $H^1(J_0(\mathfrak{n})_{\overline{F}}, \mathbb{Q}_l)$  which is faithful. If the quotient  $\mathbb{T}(\mathfrak{n})/\mathfrak{E}(\mathfrak{n})$  is not finite then for every prime ideal  $\mathfrak{q} \nmid \mathfrak{n}$  which does not divide  $\mathfrak{n}$  the element  $T_{\mathfrak{p}} - q^{\deg(\mathfrak{p})} - 1$  generates a non-trivial ideal in the  $\mathbb{Q}_l$ -algebra generated by  $T_{\mathfrak{q}}$  considered as an endomorphism of the vector space  $H^1(J_0(\mathfrak{n})_{\overline{F}}, \mathbb{Q}_l)$  by the above. Hence  $T_{\mathfrak{p}} - q^{\deg(\mathfrak{p})} - 1$  divides the minimal polynomial of the endomorphism  $T_{\mathfrak{q}}$ . In particular  $q^{\deg(\mathfrak{p})} + 1$  is an eigenvalue of this operator. Let  $\mathcal{J}_0(\mathfrak{n})$  denote the Néron model of  $J_0(\mathfrak{n})$  over  $X$ . It is known that  $\mathcal{J}_0(\mathfrak{n})$  has good reduction over all primes  $\mathfrak{q}$  which does not divide  $\mathfrak{n}$ . Let  $\text{Frob}_{\mathfrak{q}}$  denote the Frobenius endomorphism of the fiber of  $\mathcal{J}_0(\mathfrak{n})$  over the closed point  $\mathfrak{q}$ . By the Néron property the Hecke operator  $T_{\mathfrak{q}}$  induces an endomorphism of  $\mathcal{J}_0(\mathfrak{n})$ . It is known that the restriction of the latter to the fiber over  $\mathfrak{q}$  satisfies the Eichler-Shimura relation:

$$\text{Frob}_{\mathfrak{q}}^2 - T_{\mathfrak{q}} \cdot \text{Frob}_{\mathfrak{q}} + q^{\deg(\mathfrak{q})} = 0.$$

These endomorphisms induce  $\mathbb{Q}_l$ -linear operators on the étale cohomology group  $H^1(\mathcal{J}_0(\mathfrak{n})_{\mathfrak{q}}, \mathbb{Q}_l)$  where  $\mathcal{J}_0(\mathfrak{n})_{\mathfrak{q}}$  denotes the base change of the fiber of  $\mathcal{J}_0(\mathfrak{n})$  over the closed point  $\mathfrak{q}$  to the algebraic closure of the field of definition. By the proper base change theorem there is a  $T_{\mathfrak{q}}$ -equivariant isomorphism between the vector spaces  $H^1(\mathcal{J}_0(\mathfrak{n})_{\mathfrak{q}}, \mathbb{Q}_l)$  and  $H^1(J_0(\mathfrak{n})_{\overline{F}}, \mathbb{Q}_l)$  hence the action of  $T_{\mathfrak{q}}$  on  $H^1(\mathcal{J}_0(\mathfrak{n})_{\mathfrak{q}}, \mathbb{Q}_l)$  has eigenvalue  $q^{\deg(\mathfrak{p})} + 1$ . Therefore either 1 or  $q^{\deg(\mathfrak{q})}$  is an eigenvalue of the operator corresponding to  $\text{Frob}_{\mathfrak{q}}$  by the Eichler-Shimura relation above. But the latter is impossible by Weil's purity theorem if  $\deg(\mathfrak{q})$  is sufficiently large.  $\square$

**Definition 4.3.** Recall that for every pair of integers  $k, m$  a holomorphic function  $f : \Omega \rightarrow \mathbb{C}_{\infty}$  is called a Drinfeld modular form of weight  $k$ , of type  $m$  and of level  $\mathfrak{n}$  if we have

$$f(\gamma z) = (\det \gamma)^{-m} (cz + d)^k f(z) \quad (\forall z \in \Omega, \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\mathfrak{n})),$$

and  $f$  is holomorphic at the cusps. (For an explanation of the latter condition see 2.8.3 of [12], page 46). Also recall that a Drinfeld modular is called double-cuspidal

if its order of vanishing at every cusp is at least two (see 2.8.5 of [12], page 46). Let  $M_{2,1}^2(\Gamma_0(\mathfrak{n}))$  denote the space of double-cuspidal, weight two Drinfeld modular forms of type 1 and level  $\mathfrak{n}$ . Let  $X_{\mathbb{C}_\infty}$  denote the base change of any algebraic variety  $X$  over  $F$  to the spectrum of  $\mathbb{C}_\infty$ . For every differential form  $\omega \in \Gamma(X_0(\mathfrak{n})_{\mathbb{C}_\infty}, \Omega^1)$  the pull-back of the restriction  $\omega|_{Y_0(\mathfrak{n})_{\mathbb{C}_\infty}}$  via the uniformization map of Theorem 3.6 can be written as  $f_\omega(z)dz$  where  $f_\omega$  is an element of  $M_{2,1}^2(\Gamma_0(\mathfrak{n}))$ . According to Proposition 2.10.2 of [12] on page 47 the map  $\Gamma(X_0(\mathfrak{n})_{\mathbb{C}_\infty}, \Omega^1) \rightarrow M_{2,1}^2(\Gamma_0(\mathfrak{n}))$  given by the rule  $\omega \mapsto f_\omega$  is an isomorphism of vector spaces over  $\mathbb{C}_\infty$ . The vector space  $\Gamma(X_0(\mathfrak{n})_{\mathbb{C}_\infty}, \Omega^1)$  is canonically isomorphic to the  $\mathbb{C}_\infty$ -dual of the tangent space of  $J_0(\mathfrak{n})_{\mathbb{C}_\infty}$  at the identity of this group scheme hence it is equipped with an action of the algebra  $\mathbb{T}'(\mathfrak{n})$ . The corresponding action on  $M_{2,1}^2(\Gamma_0(\mathfrak{n}))$  has a description similar to the one in Definition 4.4.

**Theorem 4.4.** *There is an  $\mathbb{C}_\infty$ -vectorspace isomorphism:*

$$\text{res} : M_{2,1}^2(\Gamma_0(\mathfrak{n})) \rightarrow H_{!!}(\mathcal{T}, \mathbb{C}_\infty)^{\Gamma_0(\mathfrak{n})}$$

*such that  $\text{res}(T_q(f)) = T_q(\text{res}(f))$  for every  $f \in M_{2,1}^2(\Gamma_0(\mathfrak{n}))$  and proper prime ideal  $q \triangleleft \mathbf{A}$  not dividing  $\mathfrak{n}$ .*

**Proof.** This is Theorem 6.5.3 of [7] on page 75.  $\square$

The aim of this section is to prove the following

**Theorem 4.5.** *The number  $p$  is not an Eisenstein prime for  $\mathfrak{n}$  when  $\mathfrak{n}$  is a square-free ideal.*

According to claim (vi) of Proposition 7.11, pages 160-161 and (the proof of Corollary 11.8, pages 194-195 of [19], the number  $|\mathbb{T}(\mathfrak{p})/\mathfrak{E}(\mathfrak{p})|$  is the product of  $N(\mathfrak{p})$  and a power of  $p$  when  $\mathfrak{p}$  is a prime ideal. Hence the result above implies Theorem 1.2. Let  $M_{2,1}^{2,\text{new}}(\Gamma_0(\mathfrak{n}))$  denote the subspace of  $M_{2,1}^2(\Gamma_0(\mathfrak{n}))$  corresponding to the  $\mathbb{C}_\infty$ -dual of the tangent space of  $J_0^{\text{new}}(\mathfrak{n})_{\mathbb{C}_\infty}$ , which is a subspace of the  $\mathbb{C}_\infty$ -dual of the tangent space of  $J_0(\mathfrak{n})_{\mathbb{C}_\infty}$ , under the identification in Definition 4.3 and let  $H_{!!}^{\text{new}}(\mathcal{T}, \mathbb{C}_\infty)^{\Gamma_0(\mathfrak{n})}$  denote its image in  $H_{!!}(\mathcal{T}, \mathbb{C}_\infty)^{\Gamma_0(\mathfrak{n})}$  with respect to the map  $\text{res}$  of Theorem 4.4. The vector space  $H_{!!}^{\text{new}}(\mathcal{T}, \mathbb{C}_\infty)^{\Gamma_0(\mathfrak{n})}$  has a purely combinatorial description as the image of certain new forms under the canonical map  $H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{n})} \otimes \mathbb{C}_\infty \rightarrow H_1(\mathcal{T}, \mathbb{C})^{\Gamma_0(\mathfrak{n})}$  whose details are left to the dedicated reader. According to the discussion above Theorem 4.5 also has the following immediate

**Corollary 4.6.** *There is no non-zero element of the vector space  $M_{2,1}^{2,\text{new}}(\Gamma_0(\mathfrak{n}))$  or  $H_{!!}^{\text{new}}(\mathcal{T}, \mathbb{C}_\infty)^{\Gamma_0(\mathfrak{n})}$  fixed by the Hecke operator  $T_q$  for every proper prime ideal  $q \triangleleft \mathbf{A}$  not dividing  $\mathfrak{n}$ .  $\square$*

The claim about  $H_{!!}^{\text{new}}(\mathcal{T}, \mathbb{C}_\infty)^{\Gamma_0(\mathfrak{n})}$  in the corollary above is of elementary nature about an essentially combinatorial object but its proof is not at all elementary nor combinatorial.

**Definition 4.7.** Let  $R$  be an order of an algebraic number field  $K$ . For every abelian variety  $A$  defined over a field  $\mathbf{k}$  and for every prime number  $l$  different from the characteristic of  $\mathbf{k}$  let  $T_l(A)$  denote the  $l$ -th Tate module of  $A$  and let  $V_l(A)$  denote the vector space  $T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ . We say that  $A$  is equipped with

$R$ -multiplication  $\phi$  over the field  $\mathbf{k}$  if  $\phi : R \rightarrow \text{End}_{\mathbf{k}}(A)$  is a non-zero ring homomorphism. In this case the induced  $R$ -action on  $T_l(A)$  makes  $V_l(A)$  a free module over  $K \otimes_{\mathbb{Q}} \mathbb{Q}_l = R \otimes_{\mathbb{Z}} \mathbb{Q}_l$  of finite rank. If  $\mathbf{k}$  is a finite field then the action of the (arithmetic) Frobenius on  $V_l(A)$  is  $K \otimes_{\mathbb{Q}} \mathbb{Q}_l$ -linear, the characteristic polynomial of this action lies in  $K[t] \subset K \otimes_{\mathbb{Q}} \mathbb{Q}_l[t]$  and it is independent of the choice of  $l$ . Assume now that  $A$  is defined over  $F$  and let  $\mathcal{A}$  and  $\mathcal{A}_x$  be the Néron model of  $A$  over  $\mathbb{P}_{\mathbb{F}_q}^1$  and the fiber of  $\mathcal{A}$  over any closed point  $x$  of  $\mathbb{P}_{\mathbb{F}_q}^1$ , respectively. Let  $a_x(A) \in K$  denote coefficient of  $t$  in the characteristic polynomial  $(t) \in K[t]$  of the Frobenius on  $V_l(\mathcal{A}_x)$  for every place  $x$  of  $F$  where  $A$  has good reduction. Proper prime ideals of  $\mathbf{A}$  and the places of  $F$  different from  $\infty$  are in a natural bijective correspondence. These two sets will be identified in all that follows.

Assume that  $\pi : \mathbb{T}(\mathfrak{n}) \rightarrow R$  is a surjective ring homomorphism onto the order  $R$ .

**Theorem 4.8.** *There is an abelian variety  $A$  over  $F$  equipped with  $R$ -multiplication  $\phi$  over  $F$  such that*

- (i) *the abelian variety  $A$  is the quotient of  $J_0^{\text{new}}(\mathfrak{n})$ ,*
- (ii) *the dimension of  $A$  is equal to the rank of  $R$  as a free  $\mathbb{Z}$ -module,*
- (iii) *we have  $a_{\mathfrak{q}}(A) = \pi(T_{\mathfrak{q}})$  for every prime ideal  $\mathfrak{q} \triangleleft \mathbf{A}$  which does not divide  $\mathfrak{n}$ .*

Note that  $A$  has good reduction at every prime ideal  $\mathfrak{q} \triangleleft \mathbf{A}$  which does not divide  $\mathfrak{n}$  by condition (i) hence condition (iii) is meaningful.

**Proof.** This result is just a reformulation of the Langlands correspondence proved in the classical paper [4]. For a detailed discussion see [12].  $\square$

**Proof of Theorem 4.5.** Assume that  $p$  is an Eisenstein prime and let  $\mathfrak{P} \triangleleft \mathbb{T}(\mathfrak{n})$  be a proper minimal prime ideal which is contained in the ideal  $(\mathfrak{E}(\mathfrak{n}), p)$ . Let  $R$  denote  $\mathbb{T}(\mathfrak{n})/\mathfrak{P}$  and let  $\pi : \mathbb{T}(\mathfrak{n}) \rightarrow R$  be the quotient map. Then  $R$  is an order in a number field hence there is an abelian variety  $A$  over  $F$  with the properties described in Theorem 4.8. The image of the ideal  $(\mathfrak{E}(\mathfrak{n}), p)$  with respect to  $\pi$  is a maximal ideal  $\mathfrak{m}$  in  $R$  such that  $R/\mathfrak{m} = \mathbb{F}_p$ . For every prime ideal  $\mathfrak{q} \triangleleft \mathbf{A}$  which does not divide  $\mathfrak{n}$  we have

$$a_{\mathfrak{q}}(A) = \pi(T_{\mathfrak{q}}) \equiv q^{\deg(\mathfrak{q})} + 1 \equiv 1 \pmod{\mathfrak{m}}$$

by condition (iii). Therefore  $A$  has ordinary good reduction at every prime ideal  $\mathfrak{q} \triangleleft \mathbf{A}$  which does not divide  $\mathfrak{n}$  by Lemma 4.9 below. On the other hand  $J_0^{\text{new}}(\mathfrak{n})$  has multiplicative reduction at  $\infty$  and every prime ideal  $\mathfrak{q}$  dividing  $\mathfrak{n}$  hence so does the abelian variety  $A$ . But it should have good reduction everywhere by Theorem 2.7 which is a contradiction.  $\square$

**Lemma 4.9.** *Let  $R$  be an order in a number field  $K$ , let  $\mathfrak{m} \triangleleft R$  be an ideal such that  $R/\mathfrak{m} = \mathbb{F}_p$  and let  $A$  be an abelian variety equipped with  $R$ -multiplication  $\phi$  over a finite field  $\mathbf{k}$  of characteristic  $p$  such that the dimension of  $A$  is equal to the  $\mathbb{Z}$ -rank of  $R$ . If the coefficient of  $t$  in the characteristic polynomial  $f(t) \in K[t]$  of the Frobenius on  $V_l(A)$  lies in  $R - \mathfrak{m}$  then  $A$  is ordinary.*

**Proof.** The abelian variety  $A$  is ordinary if and only if the multiplicity of the slope 0 of the Dieudonné-crystal  $\mathbb{M}$  attached to the  $p$ -divisible group of  $A$  is equal to the dimension of  $A$ . Let  $L$  denote the field of fractions of the Witt vectors  $\mathbb{W}(\mathbf{k})$  of  $\mathbf{k}$  of infinite length. The  $R$ -multiplication  $\phi$  induces an  $R$ -action on  $\mathbb{M}$  which makes

$\mathbb{M} \otimes_{\mathbb{W}(\mathbf{k})} L$  a free module over  $K \otimes_{\mathbb{Q}} L = R \otimes_{\mathbb{Z}} \mathbb{W}(\mathbf{k})$  of rank two. The action of the  $L$ -linear Frobenius on  $\mathbb{M} \otimes_{\mathbb{W}(\mathbf{k})} L$  is  $K \otimes_{\mathbb{Q}} L$ -linear and the characteristic polynomial of this action is  $f(t)$  by the Weil conjectures. By assumption exactly one of the two roots of  $f(t)$  has valuation 0 as an element of the separable closure of  $L$ . The  $L$ -dimension of the free  $K \otimes_{\mathbb{Q}} L$ -eigenspace of this eigenvalue is equal to the dimension of  $A$  since the latter is equal to the dimension of  $K$  as a  $\mathbb{Q}$ -vectorspace by assumption. This subspace is left invariant by the absolute Frobenius and its only slope is zero. The claim is now clear.  $\square$

## 5. MODULAR SYMBOLS

**Definition 5.1.** A path  $\gamma$  on an oriented graph  $G$  is a sequence of edges

$$\{\dots, e_1, e_2, \dots, e_n, \dots\} \in \mathcal{E}(G)$$

indexed by the set  $I$  where  $I = \mathbb{Z}$ ,  $I = \mathbb{N}$  or  $I = \{0, 1, \dots, m\}$  for some  $m \in \mathbb{N}$  such that  $t(e_i) = o(e_{i+1})$  for every  $i$ ,  $i+1 \in I$ . We say that  $\gamma$  is an infinite path, a half-line or a finite path whether we are in the first, in the second or in the third case, respectively. For each edge  $e \in \mathcal{E}(G)$  let  $i_e : \mathcal{E}(G) \rightarrow \mathbb{Z}$  denote the unique function such that

$$i_e(f) = \begin{cases} +1, & \text{if } f = e, \\ -1, & \text{if } f = \bar{e}, \\ 0, & \text{otherwise.} \end{cases}$$

Let  $\gamma$  be a path  $\{\dots, e_1, \dots, e_n, \dots\}$  on  $G$  such that every edge in  $\mathcal{E}(G)$  is only listed finitely many times in the sequence above. Then the function  $i_\gamma = \sum_{j \in \mathbb{Z}} i_{e_j}$  is well-defined as the sum above has only finitely many terms non-zero on  $e$  for every edge  $e \in \mathcal{E}(G)$ . Let us consider now the special case  $G = \Gamma \backslash \mathcal{T}$  where  $\Gamma = \Gamma_0(\mathbf{n})$  is a short-hand notation introduced for convenience. Let  $z(\Gamma)$  denote the cardinality of the center of  $\Gamma$  and  $\Gamma_e$  is the stabilizer of the edge  $e \in \mathcal{E}(\mathcal{T})$  in  $\Gamma$ . (It is well-known that the latter is finite.) For every path  $\gamma$  on the graph  $\Gamma \backslash \mathcal{T}$  such that  $i_\gamma$  is defined in the sense above we define the function  $\gamma^* : \mathcal{E}(\mathcal{T}) \rightarrow \mathbb{Z}$  given by the rule  $\gamma^*(e) = |\Gamma_e| i_\gamma(\tilde{e}) / z(\Gamma)$ , where  $\tilde{e}$  is the image of the edge  $e$  in  $\mathcal{E}(\Gamma \backslash \mathcal{T})$  and the absolute sign  $|\cdot|$  denotes the cardinality of every finite set. (Since the center of  $\Gamma$  leaves the Bruhat-Tits tree invariant, it lies in the stabilizer  $\Gamma_e$ , therefore the expression above is indeed an integer.)

**Definition 5.2.** Next we are going to define the fundamental arch connecting two different points  $a, b \in \mathbb{P}^1(F_\infty)$  on the Bruhat-Tits tree. We say that a path  $\{\dots, e_1, \dots, e_n, \dots\}$  indexed by the set  $I$  on an oriented graph  $G$  is without backtracking if  $\bar{e}_i \neq e_{i+1}$  for every  $i$ ,  $i+1 \in I$ . Let  $S(a, b)$  denote the set of those edges of  $\mathcal{T}$  which can be represented by a matrix  $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$  such that the homogeneous coordinates  $(\alpha : \gamma) = a$  and  $(\beta : \delta) = b$ . The elements of the set  $S(a, b)$  can be indexed uniquely by the set of integers such that it becomes an infinite path without backtracking: this is the fundamental arch  $\overline{ab}$  connecting  $a$  and  $b$ . Let  $\overline{ab}$  denote the image of the fundamental arch under the canonical map  $\mathcal{T} \rightarrow \Gamma_0(\mathbf{n}) \backslash \mathcal{T}$  as well by slight abuse of notation. Let  $[a, b] : \mathcal{E}(\mathcal{T}) \rightarrow \mathbb{Z}$  denote the function  $(\overline{ab})^*$  introduced in Definition 5.1 if the latter is well-defined.

Let  $\mathfrak{p} \triangleleft \mathbf{A}$  be now a proper non-zero prime ideal.

**Proposition 5.3.** *The following holds:*

- (i) *for every different  $a, b \in \mathbb{P}^1(F)$  the function  $[a, b]$  is well-defined and it is a  $\mathbb{Z}$ -valued left  $\Gamma_0(\mathfrak{p})$ -invariant harmonic cochain,*
- (ii) *we have  $[a, b] \in H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$  for every different  $a, b \in \mathbb{P}^1(F)$  which are equivalent under the Möbius action of  $\Gamma_0(\mathfrak{p})$ ,*
- (iii) *for every proper non-zero prime ideal  $\mathfrak{p} \neq \mathfrak{q} \triangleleft \mathbf{A}$  we have*

$$(1 + q^{\deg(\mathfrak{q})} - T_{\mathfrak{q}})[0, \infty] \in (q - 1)H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}.$$

**Proof.** We say that two half-lines on an oriented graph are equivalent if they only differ in a finite graph. We also say that a half-line on  $\mathcal{T}$  is  $F$ -rational if it is without backtracking and it is contained in a fundamental arch  $\overline{ab}$  for some  $a, b \in \mathbb{P}^1(F)$ . By Serre's structure theorem the graph  $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$  is the union of a finite graph and finitely many half-lines. Moreover every  $F$ -rational half-line on  $\mathcal{T}$  is equivalent to a half-line  $\gamma$  such that the restriction of the projection  $\mathcal{E}(\mathcal{T}) \rightarrow \mathcal{E}(\Gamma_0(\mathfrak{p}) \backslash \mathcal{T})$  onto  $\gamma$  is a bijection onto one of those half-lines above. In particular the functions introduced in Definition 5.1 are all well-defined for the image of every  $F$ -rational half-line under the projection above. For every  $a, b \in \mathbb{P}^1(F)$  there are two half-lines  $\alpha$  and  $\beta$  on  $\mathcal{T}$  such that the disjoint union of  $\alpha$  and the set we get from  $\beta$  by reversing each of its edges is equal to  $\overline{ab}$  as a set. Let  $\alpha$  and  $\beta$  also denote the image of  $\alpha$  and  $\beta$  under the canonical map  $\mathcal{T} \rightarrow \Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ , respectively. Then  $i_{\overline{ab}} = i_{\alpha} - i_{\beta}$  as functions on  $\mathcal{E}(\Gamma_0(\mathfrak{p}) \backslash \mathcal{T})$ . Hence the function  $[a, b]$  is well-defined. Since  $\gamma^*$  is a harmonic cochain for every infinite path  $\gamma$  on  $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$  whenever the former is defined, we get that claim (i) is true. If  $a$  and  $b$  are equivalent under the Möbius action of  $\Gamma_0(\mathfrak{p})$  then the half-lines  $\alpha$  and  $\beta$  on  $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$  are equivalent hence the difference  $i_{\alpha} - i_{\beta}$  is supported on a finite set. Therefore claim (ii) is also true. We continue with the proof of part (iii). Let  $r$  be the unique monic polynomial generating  $\mathfrak{q}$ . Let  $R(\mathfrak{q}) \subset \mathbb{F}_q[T]$  denote the set of non-zero polynomials whose degree is less than  $\deg(\mathfrak{q})$  and let  $R(\mathfrak{q}, \mathfrak{p})$  denote the set

$$R(\mathfrak{q}, \mathfrak{p}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} r & a \\ 0 & 1 \end{pmatrix} \mid a \in R(\mathfrak{q}) \right\}.$$

Then the set  $R(\mathfrak{q}, \mathfrak{p})$  is a set of representatives of the double coset  $H(\mathfrak{q}, \mathfrak{p})$  introduced in Definition 3.4 as the notation indicates. For every  $e \in \mathcal{E}(\mathcal{T})$  we have:

$$\begin{aligned} T_{\mathfrak{q}}([0, \infty])(e) &= \frac{1}{z(\Gamma)} \sum_{M \in R(\mathfrak{q}, \mathfrak{p})} (|\{\gamma \in \Gamma \mid e \in M\gamma[0, \infty]\}| - |\{\gamma \in \Gamma \mid \overline{e} \in M\gamma[0, \infty]\}|) \\ &= \frac{1}{z(\Gamma)} \sum_{M \in R(\mathfrak{q}, \mathfrak{p})} (|\{\gamma \in \Gamma \mid e \in \gamma M[0, \infty]\}| - |\{\gamma \in \Gamma \mid \overline{e} \in \gamma M[0, \infty]\}|) \\ &= 2[0, \infty] + \sum_{0 \neq a \in R(\mathfrak{q})} [a/r, \infty] \end{aligned}$$

using again the notation  $\Gamma = \Gamma_0(\mathfrak{p})$  of Definition 5.1. The first equation above is just the definition. The second equation follows from the fact that every product  $M\gamma$  where  $M \in R(\mathfrak{q})$  and  $\gamma \in \Gamma_0(\mathfrak{p})$  can be written uniquely as a product  $\gamma'M'$  for some  $M' \in R(\mathfrak{q})$  and  $\gamma' \in \Gamma_0(\mathfrak{p})$ . The last equation follows from the fact that

for every  $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(F)$  the image of the fundamental arch  $\overline{0\infty}$  under the automorphism of  $\mathcal{T}$  induced by multiplication on the left by the matrix  $M$  is the fundamental arch  $\overline{(\beta : \delta)(\alpha : \gamma)}$ . Note that for every  $a, b$  and  $c \in \mathbb{P}^1(F)$  which are pair-wise different we have  $[a, b] = [a, c] + [c, b]$ . Therefore

$$(1 + q^{\deg(\mathfrak{q})} - T_{\mathfrak{q}})[0, \infty] = \sum_{0 \neq a \in R(\mathfrak{q})} [0, a/r].$$

Note that for every  $0 \neq a \in R(\mathfrak{q})$  the polynomials  $r$  and  $a$  are relatively prime hence there are polynomials  $c, d \in \mathbf{A}$  such that the matrix  $\begin{pmatrix} c & a \\ d & r \end{pmatrix}$  is an element of  $\Gamma_0(\mathfrak{p})$ . This matrix maps  $0$  to  $a/r$  via the Möbius action so  $[0, a/r] \in H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$  by claim (ii). Since  $[0, a/r] = [0, ca/r]$  for every  $a \in R(\mathfrak{q})$  and every  $c \in \mathbb{F}_q^*$  the equation above implies claim (iii).  $\square$

**Definition 5.4.** Recall that a finite path  $\{e_0, e_2, \dots, e_n\} \in \mathcal{E}(G)$  on an oriented graph  $G$  is closed if the equality  $t(e_n) = o(e_0)$  holds, too. We define  $H_1(G, \mathbb{Z})$  as the abelian group of  $\mathbb{Z}$ -valued functions on  $\mathcal{E}(G)$  generated by the functions  $i_\gamma$  where  $\gamma$  is a closed path. We define the map

$$j_{\Gamma_0(\mathfrak{n})} : H_1(\Gamma_0(\mathfrak{n}) \backslash \mathcal{T}, \mathbb{Z}) \rightarrow H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{n})},$$

as the unique homomorphism which maps  $i_\gamma$  to the cochain  $\gamma^*$  for every  $\gamma$  closed path, using the notations of Definition 5.1. It is easy to see that the homomorphism is well-defined, that is  $\gamma^*$  is indeed a harmonic cochain. By a theorem of Gekeler and Nonnengardt (Theorem 3.3 of [11], page 702) this homomorphism is in fact an isomorphism.

**Definition 5.5.** Let  $\Gamma_0(\mathfrak{p})_{\text{ab}} = \Gamma_0(\mathfrak{p})/[\Gamma_0(\mathfrak{p}), \Gamma_0(\mathfrak{p})]$  be the abelianization of  $\Gamma_0(\mathfrak{p})$ , and let  $\overline{\Gamma}_0(\mathfrak{p}) = \Gamma_0(\mathfrak{p})_{\text{ab}}/(\Gamma_0(\mathfrak{p})_{\text{ab}})_{\text{tors}}$  be its maximal torsion-free quotient. For each  $\gamma \in \Gamma_0(\mathfrak{p})$  let  $\overline{\gamma}$  denote its image in  $\overline{\Gamma}_0(\mathfrak{p})$ . Fix a vertex  $v_0 \in \mathcal{V}(\mathcal{T})$  and for every  $\gamma \in \Gamma_0(\mathfrak{p})$  let  $e_0, e_1, \dots, e_{n(\gamma)}$  be the unique geodesic path connecting  $v_0$  with  $\gamma(v_0)$ , that is  $v_0 = o(e_1)$  and  $\gamma(v_0) = t(e_{n(\gamma)})$ . Recall that a path is geodesic if it is the shortest connecting its endpoints, in this case  $v_0$  with  $\gamma(v_0)$ , i.e. the number  $n(\gamma)$  is the smallest possible. The image of the path  $e_0, e_1, \dots$  is closed in  $\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}$ : let  $i(\gamma)$  denote the corresponding element in  $H_1(\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}, \mathbb{Z})$ . The function  $i$  induces a homomorphism  $i : \overline{\Gamma}_0(\mathfrak{p}) \rightarrow H_1(\Gamma_0(\mathfrak{p}) \backslash \mathcal{T}, \mathbb{Z})$  which is independent of the choice of  $v_0$  and it is an isomorphism. We will use this identification without further notice.

Let  $\Phi_{AJ} : \text{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*) \rightarrow J_0(\mathfrak{p})(\mathbb{C}_\infty)$  be the Abel-Jacobi map of Gekeler-Reversat. (For a description using the same notation see sections 7.1-7.7 of [19] on pages 158-159.) It is a group homomorphism holomorphic in the rigid analytic sense. Let  $c : \overline{\Gamma}_0(\mathfrak{p}) \rightarrow \text{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$  be the period map defined in Proposition 7.5 of [19] on page 159. Note that the domain of the map  $c$  is equipped with an action of the operator  $T_{\mathfrak{q}}$  via the isomorphism  $j_{\Gamma_0(\mathfrak{p})}$ . The following result is Theorem 7.9 of [19] on page 139.

**Theorem 5.6.** *For every prime  $\mathfrak{q} \triangleleft \mathbf{A}$ , different from  $\mathfrak{p}$ , there is a unique endomorphism  $T_{\mathfrak{q}}$  of the rigid analytic torus  $\text{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$ , which leaves the lattice  $\overline{\Gamma}_0(\mathfrak{p})$  invariant, and makes the diagram:*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \overline{\Gamma}_0(\mathfrak{p}) & \xrightarrow{c} & \text{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*) & \xrightarrow{\Phi_{AJ}} & J_0(\mathfrak{p})(\mathbb{C}_\infty) \longrightarrow 0 \\ & & T_{\mathfrak{q}} \downarrow & & T_{\mathfrak{q}} \downarrow & & T_{\mathfrak{q}} \downarrow \\ 0 & \longrightarrow & \overline{\Gamma}_0(\mathfrak{p}) & \xrightarrow{c} & \text{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*) & \xrightarrow{\Phi_{AJ}} & J_0(\mathfrak{p})(\mathbb{C}_\infty) \longrightarrow 0 \end{array}$$

commutative. Moreover the map  $j : \bar{\Gamma}_0(\mathfrak{p}) \rightarrow \mathcal{H}_0(\mathfrak{p}, \mathbb{Z})$  is equivariant with respect to this action on  $\bar{\Gamma}_0(\mathfrak{p})$  and the action of the Hecke operator  $T_q$  on  $\mathcal{H}_0(\mathfrak{p}, \mathbb{Z})$ .  $\square$

**Remarks 5.7.** For the moment let  $\mathbb{T}(\mathfrak{p})'$  denote the ring with unity generated by the operators  $T_q$  acting on the torus  $\text{Hom}(\bar{\Gamma}_0(\mathfrak{p}), \mathbb{C}_\infty^*)$ . The rigid analytic endomorphisms of algebraic tori are algebraic, so they act faithfully on any Zariski-dense invariant subset. In particular the action of  $\mathbb{T}(\mathfrak{p})'$  on the module  $\bar{\Gamma}_0(\mathfrak{p})$  is faithful. Since  $\Phi_{AJ}$  injects  $\text{Hom}(\bar{\Gamma}_0(\mathfrak{p}), \mathcal{O}_\infty^*)$  into  $J_0(\mathfrak{p})(F_\infty)$ , the action of  $\mathbb{T}(\mathfrak{p})'$  on the Jacobian  $J_0(\mathfrak{p})$  is also faithful. Therefore the algebra  $\mathbb{T}(\mathfrak{p})'$  is canonically isomorphic to the Hecke algebra  $\mathbb{T}(\mathfrak{p})$  introduced in Definition 4.1. In particular we have a well-defined homomorphism

$$e : \mathfrak{E}(\mathfrak{p}) \rightarrow H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$$

of  $\mathbb{T}(\mathfrak{p})$ -modules given by the rule  $\alpha \mapsto \alpha([0, \infty])/(q-1)$  according to part (iii) of Proposition 5.3. This map is the analogue of the winding homomorphism introduced by Mazur.

**Definition 5.8.** Let  $B$  denote the group scheme of invertible upper triangular two by two matrices. Let  $h : \Gamma_0(\mathfrak{p}) \rightarrow \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}$  denote the composition of the reduction map  $r : \Gamma_0(\mathfrak{p}) \rightarrow B(\mathbf{A}/\mathfrak{p}) \subset GL_2(\mathbf{A}/\mathfrak{p}) \bmod \mathfrak{p}$ , the upper left conner element  $a : B(\mathbf{A}/\mathfrak{p}) \rightarrow (\mathbf{A}/\mathfrak{p})^*$  and the surjection  $s : (\mathbf{A}/\mathfrak{p})^* \rightarrow \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}$  which is unique up to isomorphism. This homomorphism factors through  $\bar{\Gamma}_0(\mathfrak{p})$ , so it induces a homomorphism:

$$\phi = h \circ j_{\Gamma_0(\mathfrak{p})}^{-1} : H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})} \rightarrow \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}$$

under the identification of Definition 5.5.

**Lemma 5.9.** *The kernel of  $\phi$  contains  $\mathfrak{E}(\mathfrak{p})H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$  and induces an isomorphism*

$$\bar{\phi} : H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})} / \mathfrak{E}(\mathfrak{p})H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})} \rightarrow \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}.$$

**Proof.** Let  $\mu_\infty \subset \mathbb{C}_\infty^*$  denote the subgroup of the roots of unity. Under the map  $\Psi_{AJ}$  of Theorem 5.6 the image of  $\text{Hom}(\bar{\Gamma}_0(\mathfrak{p}), \mu_\infty)$  maps isomorphically onto the group of those torsion points of  $J_0(\mathfrak{p})(\mathbb{C}_\infty)$  which are defined over the maximal unramified extension  $K_\infty$  of  $F_\infty$  and map into the connected component of the identity of the special fiber of the Néron model of  $J_0(\mathfrak{p})$  over the valuation ring of  $K_\infty$  under the specialization map. By Theorem 1.2 the prime  $p$  does not divide the order of  $\mathbb{T}(\mathfrak{p})/\mathfrak{E}(\mathfrak{p})$  hence the quotient  $H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})} / \mathfrak{E}(\mathfrak{p})H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$  is dual to the part of  $\text{Hom}(\bar{\Gamma}_0(\mathfrak{p}), \mu_\infty)$  annihilated by the Eisenstein ideal. There is a unique subgroup of  $\mu_\infty$  isomorphic to  $\mathbb{Z}/N(\mathfrak{p})\mathbb{Z}$  hence the homomorphism  $\phi$  can be considered as an element of  $\text{Hom}(\bar{\Gamma}_0(\mathfrak{p}), \mu_\infty)$ . During the proof of claim (i) of Proposition 8.18 of [19], pages 171-172, we also showed incidentally that the subgroup generated by  $\phi$  is the Shimura group  $\mathcal{S}(\mathfrak{p})$  introduced in the paper quoted above. On the other hand some of the main results of this paper, in particular Theorem 10.5 on page 187 and Corollary 11.8 on pages 194-195 imply that the Shimura group is the largest subgroup of  $\text{Hom}(\bar{\Gamma}_0(\mathfrak{p}), \mu_\infty)$  annihilated by the Eisenstein ideal.  $\square$

For every element  $b \in \mathbf{A}$  let  $\bar{b} \in \mathbf{A}/\mathfrak{p}$  denote the reduction of  $b$  modulo the ideal  $\mathfrak{p}$ . The following proposition is the analogue of Mazur's congruence formula for the modular symbol:



**Proposition 5.10.** *Let  $a, b$  be relatively prime elements in  $\mathbf{A}$  with  $b$  relatively prime to  $\mathfrak{q}$ . Then*

$$\phi([0, a/b]) = s(\bar{b}) \in \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}.$$

**Proof.** By assumption there are polynomials  $c, d \in \mathbf{A}$  such that the matrix  $M = \begin{pmatrix} c & a \\ d & b \end{pmatrix}$  is an element of  $\Gamma_0(\mathfrak{p})$ . This matrix maps 0 to  $a/b$  so  $[0, a/b] \in H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$  by claim (ii) of Proposition 5.3. In particular the left hand side of the equation above is well-defined. If  $\alpha$  is a half-line on  $\mathcal{T}$  such that the set we get from  $\alpha$  by reversing each of its edges is contained in  $\overline{0(a/b)}$  then the half-line  $M\alpha$  is equivalent to a half-line contained in  $\overline{0(a/b)}$  because the images of the half-lines  $\alpha$  and  $M\alpha$  with respect to the canonical map  $\mathcal{T} \rightarrow \Gamma_0(\mathfrak{n}) \backslash \mathcal{T}$  are equivalent. Therefore there is an edge  $e \in \overline{0(a/b)}$  such that  $\overline{Me} \in \overline{0(a/b)}$ , too. Now let  $\alpha$  denote the unique half line whose first edge (indexed by zero) is  $\bar{e}$  and  $M\alpha$  is contained in  $\overline{0(a/b)}$ . Let  $\gamma$  denote the unique geodesic connecting the vertex  $o(e)$  to the vertex  $o(Me) = Mo(e)$  and let  $\gamma'$  denote its image with respect to the canonical map  $\mathcal{T} \rightarrow \Gamma_0(\mathfrak{n}) \backslash \mathcal{T}$ . Then  $\overline{0(a/b)}$  as a set is the union of  $M\alpha$ ,  $\gamma$  and set we get from  $\alpha$  by reversing each of its edges. Therefore  $(\overline{0(a/b)})^* = (\gamma')^*$  using the notation of Definition 5.1, so  $[0, a/b] = j_{\Gamma(\mathfrak{p})}(i(M))$  using the notation of Definitions 5.4 and 5.5. But  $\phi(i(M)) = s(\bar{b})$  by definition.  $\square$

For every prime  $\mathfrak{q} \triangleleft \mathbf{A}$ , different from  $\mathfrak{p}$ , let  $\bar{\mathfrak{q}} \in \mathbf{A}/\mathfrak{p}$  denote the reduction  $\overline{r(T)}$  of the unique monic polynomial  $r(T) \in \mathbf{A}$  generating the ideal  $\mathfrak{q}$  modulo the ideal  $\mathfrak{p}$ . The next claim is the analogue of Mazur's congruence formula for the winding homomorphism:

**Corollary 5.11.** *For every prime  $\mathfrak{q} \triangleleft \mathbf{A}$ , different from  $\mathfrak{p}$ , we have*

$$\phi \circ e(1 + q^{\deg(\mathfrak{q})} - T_{\mathfrak{q}}) = \frac{q^{\deg(\mathfrak{q})} - 1}{q - 1} s(\bar{\mathfrak{q}}) \in \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}.$$

**Proof.** Let  $S(\mathfrak{q}) \subset \mathbb{F}_{\mathfrak{q}}[T]$  denote the set of non-zero monic polynomials of degree less than  $\deg(\mathfrak{q})$ . According to the formula which we derived in the proof of Proposition 5.3 we have:

$$\phi \circ e(1 + q^{\deg(\mathfrak{q})} - T_{\mathfrak{q}}) = \phi\left(\sum_{a \in S(\mathfrak{q})} [0, a/r]\right) = \frac{q^{\deg(\mathfrak{q})} - 1}{q - 1} s(\bar{\mathfrak{q}}),$$

where we used Proposition 5.10 in the second equation.  $\square$

**Definition 5.12.** For the rest of this chapter we fix an Eisenstein prime  $l$  for  $\mathfrak{p}$ . We define the  $\mathbb{Z}_l$  algebra  $\mathbb{T}_l(\mathfrak{p})$  as the tensor product  $\mathbb{T}(\mathfrak{p}) \otimes \mathbb{Z}_l$  and let  $\mathfrak{P} \triangleleft \mathbb{T}_l(\mathfrak{p})$  be the unique prime ideal lying above the ideal  $\mathfrak{J}$  generated by  $\mathfrak{E}(\mathfrak{p})$  in  $\mathbb{T}_l(\mathfrak{p})$ . Let  $\mathbb{T}_{\mathfrak{P}}$  denote the completion of  $\mathbb{T}_l(\mathfrak{p})$  at the prime ideal  $\mathfrak{P}$ : this algebra is canonically isomorphic to the completion of  $\mathbb{T}(\mathfrak{p})$  at the ideal  $\mathfrak{P}(\mathfrak{p}, l)$  where  $\mathfrak{P}(\mathfrak{p}, l) \triangleleft \mathbb{T}(\mathfrak{p})$  is the unique prime ideal lying above the ideal generated by  $\mathfrak{E}(\mathfrak{p})$  and  $l$ . As  $\mathbb{Z}$  surjects onto  $\mathbb{T}(\mathfrak{p})/\mathfrak{E}(\mathfrak{p})$  via its natural inclusion into  $\mathbb{T}(\mathfrak{p})$ , clearly  $\mathfrak{P}(\mathfrak{p}, l) = (\mathfrak{E}(\mathfrak{p}), l)$ . Hence the latter is a maximal ideal with residue field  $\mathbb{F}_l$ . Let  $\eta_{\mathfrak{q}}$  denote the element  $T_{\mathfrak{q}} - q^{\deg(\mathfrak{q})} - 1 \in \mathbb{T}(\mathfrak{p})$ , where  $\mathfrak{q} \triangleleft \mathbf{A}$  is any prime ideal different from  $\mathfrak{p}$ . Now fix

such an ideal  $\mathfrak{q} \triangleleft \mathbf{A}$  and let  $r(T) \in \mathbf{A}$  denote again the unique monic polynomial which generates  $\mathfrak{q}$ . We say that  $\mathfrak{q}$  is a good prime if the element

$$\frac{q^{\deg(\mathfrak{q})} - 1}{q - 1} s(\bar{\mathfrak{q}}) \in \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}$$

is not divisible by  $l$  in the group  $\mathbb{Z}/N(\mathfrak{p})\mathbb{Z}$ . It is very easy to see that this definition is equivalent to notion we introduced in Definition 10.1 of [19] on page 186. As we already remarked there, the Chebotarev density theorem implies that there are infinitely many good primes. Let  $H_{\mathfrak{P}}$  denote the  $\mathbb{T}_{\mathfrak{P}}$ -module  $H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})} \otimes_{\mathbb{T}(\mathfrak{p})} \mathbb{T}_{\mathfrak{P}}$  and let  $e_l : \mathcal{J} \rightarrow H_{\mathfrak{P}}$  denote the tensor product  $e \otimes_{\mathbb{T}(\mathfrak{p})} \text{id}$ .

**Theorem 5.13.** *The following holds:*

- (i) *the module  $H_{\mathfrak{P}}$  is a free  $\mathbb{T}_{\mathfrak{P}}$ -module of rank one,*
- (ii) *the winding homomorphism  $e_l : \mathcal{J} \rightarrow H_{\mathfrak{P}}$  is an isomorphism,*
- (iii) *for every  $\mathfrak{q} \triangleleft \mathbf{A}$  prime ideal different from  $\mathfrak{p}$  the element  $\eta_{\mathfrak{q}}$  is a generator of the ideal  $\mathcal{J}$  if and only if  $\mathfrak{q}$  is a good prime.*

**Proof.** The module  $H_{\mathfrak{P}}$  is just the base change of the finitely generated  $\mathbb{T}_l(\mathfrak{p})$ -module  $H_1(\mathcal{T}, \mathbb{Z}_l)^{\Gamma_0(\mathfrak{p})}$  to the ring  $\mathbb{T}_{\mathfrak{P}}$ . The latter is the  $\mathbb{Z}_l$ -dual of a  $\mathbb{T}_l(\mathfrak{p})$ -module  $T_l$  introduced in Definition 7.10 of [19] on page 160. The module  $T_l$  is proved to be a locally free  $\mathbb{T}_l(\mathfrak{p})$ -module of rank one in Proposition 7.11 of the paper quoted above. Since  $\mathbb{T}_{\mathfrak{P}}$  is a Gorenstein ring over  $\mathbb{Z}_l$  by Theorems 10.2 and 11.6 of the same paper, the module  $H_{\mathfrak{P}}$  must be free of rank one as the claim (i) says above. Reducing the winding homomorphism  $e_l \bmod \mathcal{J}$  one gets a homomorphism  $\epsilon : \mathcal{J}/\mathcal{J}^2 \rightarrow H_{\mathfrak{P}}/\mathcal{J}$  and by Lemma 5.9 and Corollary 5.11 the latter maps the element  $\eta_{\mathfrak{q}}$  to a generator of  $H_{\mathfrak{P}}/\mathcal{J}$  if and only if  $\mathfrak{q}$  is a good prime. Since there are good primes the map  $e_l$  must be surjective by Nakayama's lemma. But  $e_l$  is a map between torsion-free modules whose base change to  $\mathbb{T}_l(\mathfrak{p}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$  has dimension one, so it must be an isomorphism. Hence  $\mathcal{J}$  is free and by the above and the element  $\eta_{\mathfrak{q}}$  is a generator if and only if  $\mathfrak{q}$  is a good prime.  $\square$

## 6. UNIVERSAL DEFORMATION RINGS

**Notation 6.1.** For every field  $K$  let  $\overline{K}$  and  $\text{Gal}(\overline{K}|K)$  denote the separable closure and the absolute Galois group of  $K$ , respectively. For every prime number  $l \neq p$  let  $\chi_l : \text{Gal}(\overline{F}|F) \rightarrow \mathbb{Z}_l^*$  denote the cyclotomic character and let  $\overline{\chi}_l : \text{Gal}(\overline{F}|F) \rightarrow \mathbb{F}_l^*$  denote the composition of  $\chi_l$  and the reduction  $\mathbb{Z}_l^* \rightarrow \mathbb{F}_l^* \bmod l\mathbb{Z}_l$ . Moreover let  $\overline{\phi}_l : \text{Gal}(\overline{F}|F) \rightarrow \mathbb{F}_l$  denote the unique surjective additive homomorphism unramified at every place of  $F$  such that  $\overline{\phi}_l(\text{Fr}_{\infty}) = 1$  where  $\text{Fr}_{\infty}$  is a lift of the Frobenius at the place  $\infty$  corresponding to the point at infinity on the projective line  $\mathbb{P}_{\mathbb{F}_q}^1$  over  $\mathbb{F}_q$ . Finally let  $\overline{\rho}_l : \text{Gal}(\overline{F}|F) \rightarrow GL_2(\mathbb{F}_l)$  denote the Galois representation such that

$$\overline{\rho}_l(g) = \begin{pmatrix} 1 & 0 \\ 0 & \overline{\chi}_l(g) \end{pmatrix} \quad (\forall g \in \text{Gal}(\overline{F}|F))$$

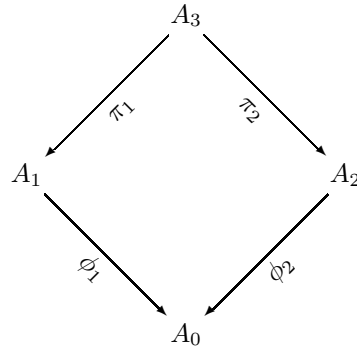
when  $l$  does not divide  $q - 1$  and

$$\overline{\rho}_l(g) = \begin{pmatrix} 1 & \overline{\phi}_l(g) \\ 0 & 1 \end{pmatrix} \quad (\forall g \in \text{Gal}(\overline{F}|F))$$

when  $l$  does divide  $q - 1$ .

**Definition 6.2.** For any commutative ring  $A$  with unity and  $A$ -module  $M$  let  $GL_A(M)$  denote the group of  $A$ -linear automorphisms of  $M$ . For any local ring  $A$  let  $\mathfrak{m}_A$  denote the maximal ideal of  $A$ . Let  $\mathbf{k}$  be a field and let  $\mathcal{O}$  be a noetherian complete local ring with residue field  $\mathbf{k}$ . let  $\mathcal{C}$  denote the category of those local Artinian  $\mathcal{O}$ -algebras such that the map  $\mathcal{O} \rightarrow A/\mathfrak{m}_A$  induced by the  $\mathcal{O}$ -structure is surjective for every object  $A$  of  $\mathcal{C}$ . Let  $G$  be a topological group. A representation of  $G$  over an object  $A$  of  $\mathcal{C}$  is an ordered pair  $(M, \rho)$  where  $M$  is a finitely generated free  $A$ -module and  $\rho$  is a continuous  $G$ -action  $\rho : G \rightarrow GL_A(M)$  where  $M$  is equipped with the discrete topology. For every object  $A$  of the category  $\mathcal{C}$  let  $\mathcal{P}_G(A)$  denote the class consisting of ordered pairs  $(V, L)$  where  $V$  is a representation  $(M, \rho)$  of  $G$  over  $A$  and  $L \subseteq M$  is a  $A$ -submodule which is a direct summand of  $M$  and it is free as an  $A$ -module. Two elements  $O = ((M, \rho), V)$  and  $O' = ((M', \rho'), L')$  of  $\mathcal{P}_G(A)$  are said to be isomorphic if there is an isomorphism  $\phi : M \rightarrow M'$  of  $A[G]$ -modules such that  $\phi(L) = L'$ . Such a relation will be denoted by  $O \cong_{A[G]} O'$ . For every morphism  $f : A \rightarrow A'$  and every element  $O = ((M, \rho), L) \in \mathcal{P}_G(A)$  let  $O \otimes_A A'$  denote the couple  $((M \otimes_A A', \rho_{A'}), L \otimes_A A')$  where  $\rho_{A'}$  is the composition of  $\rho$  and the map  $GL_A(M) \rightarrow GL_{A'}(M \otimes_A A')$  which assigns  $\phi \otimes \text{id}_{A'}$  to  $\phi \in GL_A(M)$ . Let  $O$  be an element of  $\mathcal{P}_G(\mathbf{k})$ . By a deformation of  $O$  over  $A \in \text{Ob}(\mathcal{C})$  we mean an isomorphism class of elements  $P$  of  $\mathcal{P}_G(A)$  which satisfy the condition  $P \otimes_A \mathbf{k} \cong_{\mathbf{k}[G]} O$ . Let  $\text{Def}(O, A)$  denote the set of deformations of  $O$  over  $A$ . Every morphism  $f : A \rightarrow A'$  induces a map  $f_* : \text{Def}(O, A) \rightarrow \text{Def}(O, A')$  that maps the isomorphism class of  $O \in \mathcal{P}_G(A)$  to the isomorphism class of  $O \otimes_A A' \in \mathcal{P}_G(A')$  which makes  $\text{Def}(O, \cdot)$  a covariant functor from  $\mathcal{C}$  to the category *Sets* of sets.

**Definition 6.3.** For any commutative ring  $A$  with unity let  $A[\epsilon]$  denote the  $A$ -algebra generated by  $\epsilon$  subject to the relation  $\epsilon^2 = 0$ . When  $A \in \text{Ob}(\mathcal{C})$  so does  $A[\epsilon]$ . The unique surjective  $A$ -algebra homomorphism  $a : A[\epsilon] \rightarrow A$  is called the augmentation map. For every pair of local  $\mathcal{O}$ -algebras  $A$  and  $B$  let  $\text{Hom}_{\mathcal{O}}(A, B)$  denote the  $\mathcal{O}$ -module of local  $\mathcal{O}$ -algebra homomorphisms. We say that a covariant functor  $D : \mathcal{C} \rightarrow \text{Sets}$  is pro-representable if there is a complete local  $\mathcal{O}$ -algebra  $R$  such that  $R/\mathfrak{m}_R^n$  is an object of  $\mathcal{C}$  for every natural number  $n$  and the functors  $D$  and  $\text{Hom}_{\mathcal{O}}(R, \cdot)$  are naturally isomorphic. Let  $D : \mathcal{C} \rightarrow \text{Sets}$  be a covariant functor such that  $D(\mathbf{k})$  consists of a single set and let



be a cartesian diagram of artinian rings in  $\mathcal{C}$  which means that the diagram is commutative and  $A_3$  is the fiber product  $A_1 \times_A A_2$ . Because the compositions  $D(\phi_1) \circ D(\pi_1) : D(A_3) \rightarrow D(A_0)$  and  $D(\phi_2) \circ D(\pi_2) : D(A_3) \rightarrow D(A_0)$  are equal we have a map  $h : D(A_3) \rightarrow D(A_1) \times_{D(A_0)} D(A_2)$ . Assume for a moment that

$A_1 = A_2 = \mathbf{k}[\epsilon]$  and  $\phi_1 = \phi_2$  is the augmentation map. If the morphism

$$h : D(\mathbf{k}[\epsilon] \times_{\mathbf{k}} \mathbf{k}[\epsilon]) \rightarrow D(\mathbf{k}[\epsilon]) \times D(\mathbf{k}[\epsilon])$$

is bijective then the set  $t_D = D(\mathbf{k}[\epsilon])$  is equipped with a natural  $\mathbf{k}$ -vectorspace structure according to Lemma 2.10 of [21] on page 212 and it is called the tangent space of the functor  $D$ . We say that a morphism  $h : A \rightarrow B$  of  $\mathcal{C}$  is small if it is surjective and its kernel is a principal ideal annihilated by  $\mathfrak{m}_A$ .

**Theorem (Schlessinger) 6.4.** *Let  $D : \mathcal{C} \rightarrow \text{Sets}$  be a covariant functor such that  $D(\mathbf{k})$  consists of a single set. Then  $D$  is pro-representable by a noetherian local  $\mathcal{O}$ -algebra if and only if the following conditions hold:*

- H1.** *the map  $h$  is surjective if  $\phi_1 : A_1 \rightarrow A_3$  is small,*
- H2.** *the map  $h$  is bijective if  $\phi_2 : A_1 \rightarrow A_3$  is the augmentation map  $a : \mathbf{k}[\epsilon] \rightarrow \mathbf{k}$ ,*
- H3.** *the dimension  $\dim_{\mathbf{k}}(t_D)$  is finite,*
- H4.** *the map  $h$  is bijective if  $\phi_1 : A_1 \rightarrow A_3$  and  $\phi_2 : A_2 \rightarrow A_3$  are equal and small,*

using the notation of Definition 6.3.

Note that condition **H3** makes sense because of condition **H2**.

**Proof.** This is Theorem 2.11 of [21] on pages 212-215.  $\square$

**Definition 6.5.** For every place  $x$  of  $F$  let  $D_x \subset \text{Gal}(\overline{F}|F)$  be the decomposition group at  $x$  (unique up to conjugation) and let  $I_x \triangleleft D_x$  denote its inertia subgroup. Fix a prime number  $l \neq p$  and suppose that  $\mathcal{O} = \mathbb{Z}_l$  and  $G = \text{Gal}(\overline{F}|F)$  using the notation of Definitions 6.2-6.3. Let  $O_l \in \mathcal{P}_G(\mathbb{F}_l)$  denote the couple  $((\mathbb{F}_l^2, \rho_l), \overline{L})$  where  $\overline{L} \subset \mathbb{F}_l^2$  is an affine line which is not fixed by  $\text{Gal}(\overline{F}|F)$  with respect to  $\rho_l$ . (To fix ideas, let  $\overline{L}$  be spanned by  $(1, 1)$ , when  $l \nmid q - 1$ , and let  $\overline{L}$  be spanned by  $(0, 1)$ , otherwise.) Let  $S$  be a finite subset of the set of proper prime ideals of  $\mathbf{A}$ . For every  $A \in \text{Ob}(\mathcal{C})$  let  $\text{Def}_S(A) \subseteq \text{Def}(O_l, A)$  denote the subset of isomorphism classes of those deformations  $O = ((M, \rho), L)$  of  $O_l$  which satisfy the following conditions:

- D1.** the representation  $\rho$  is unramified at every prime ideal  $\mathfrak{q} \notin S$ ,
- D2.** the inertia subgroup  $I_{\mathfrak{p}}$  at  $\mathfrak{p}$  acts trivially on the submodule  $L$ ,
- D3.** the determinant of  $\rho$  is equal to the composition  $\chi_A$  of the cyclotomic character  $\chi_l : \text{Gal}(\overline{F}|F) \rightarrow \mathbb{Z}_l^*$  and the natural map  $\mathbb{Z}_l^* \rightarrow A^*$ ,
- D4.** the  $A[D_{\infty}]$ -module  $M$  has a filtration:

$$0 \longrightarrow A(1) \longrightarrow M \longrightarrow A \longrightarrow 0$$

where  $A(1)$ ,  $A$  denotes the free  $A$ -module of rank one equipped with the  $D_{\infty}$ -action given by  $\chi_A|_{D_{\infty}}$  and the trivial character, respectively.

For every morphism  $f : A \rightarrow A'$  the function  $f_* : \text{Def}(O_l, A) \rightarrow \text{Def}(O_l, A')$  maps  $\text{Def}_S(A)$  into  $\text{Def}_S(A')$  hence  $\text{Def}_S(\cdot)$  is a sub-functor of  $\text{Def}(O_l, \cdot)$ .

The aim of the chapter is to prove theorem below with the aid of Schlessinger's criteria.

**Theorem 6.6.** *The covariant functor  $\text{Def}_S(\cdot)$  is pro-representable by a noetherian complete local  $\mathcal{O}$ -algebra.*

The noetherian complete local  $\mathbb{Z}_l$ -algebra  $R$  which pro-represents the functor  $\text{Def}_S(\cdot)$  is unique up to unique isomorphism. It is called the universal deformation ring of this functor.

**Proof.** For every  $A \in \text{Ob}(\mathcal{C})$  let  $\text{Def}'_S(A) \subseteq \text{Def}(O_l, A)$  denote the subset of isomorphism classes of those deformations  $O = ((M, \rho), L)$  of  $O_l$  which satisfy the condition **D1** above. Then  $\text{Def}_S(A) \subseteq \text{Def}'_S(A)$  and  $\text{Def}'_S(\cdot)$  is a sub-functor of  $\text{Def}(O_l, \cdot)$ .

**Lemma 6.7.** *It is sufficient to prove that the functor  $\text{Def}'_S(\cdot)$  is pro-representable by a noetherian local  $\mathcal{O}$ -algebra.*

**Proof.** The demonstration of this lemma uses the same idea as the proof of Proposition 6.1 of [2] on page 323, so we include it only for the reader's convenience. Assume that  $\text{Def}'_S(\cdot)$  is pro-representable by a noetherian local  $\mathcal{O}$ -algebra  $R$ . Then we are going to show that  $\text{Def}_S(\cdot)$  is pro-representable by a quotient  $T$  of  $R$ . For every ideal  $\mathfrak{a} \triangleleft A$  let  $\pi_{\mathfrak{a}} : A \rightarrow A/\mathfrak{a}$  denote the quotient map. Note that for every  $A \in \text{Ob}(\mathcal{C})$  and for every  $D \in \text{Def}'_S(A)$  the subset  $\text{Def}_S(A) \subseteq \text{Def}'_S(A)$  satisfies the following properties:

- (i) we have  $f_*(D) \in \text{Def}_S(B)$  for every surjective morphism  $f : A \rightarrow B$  in  $\mathcal{C}$ ,
- (ii) if  $\mathfrak{a}$  and  $\mathfrak{b}$  are proper ideals of  $A$  such that  $\pi_{\mathfrak{a}*}(D) \in \text{Def}_S(A/\mathfrak{a})$  and  $\pi_{\mathfrak{b}*}(D) \in \text{Def}_S(A/\mathfrak{b})$  then  $\pi_{\mathfrak{a} \cap \mathfrak{b}*}(D) \in \text{Def}_S(A/(\mathfrak{a} \cap \mathfrak{b}))$ ,
- (iii) if  $f : A \rightarrow B$  is an injective morphism in  $\mathcal{C}$  then we have  $D \in \text{Def}_S(A)$  if and only if  $f_*(D) \in \text{Def}_S(B)$ .

Let  $J$  denote the set of those open and closed ideals  $\mathfrak{n}$  of  $R$  such that the isomorphism class deformations of  $O_l$  over  $R/\mathfrak{n}$  corresponding to the quotient map  $R \rightarrow R/\mathfrak{n}$  lies in  $\text{Def}_S(R/\mathfrak{n})$ . Then  $J$  is closed under finite intersections by property (ii) and we have  $\mathfrak{r} \in J$  for every open and closed ideal  $\mathfrak{r}$  which contains an element of  $J$  by property (i). Let  $\mathfrak{j}$  denote the intersection of all ideals belonging to the set  $J$ : it is a closed ideal. We claim that every open and closed ideal  $\mathfrak{n}$  which contains  $\mathfrak{j}$  is an element of  $J$ . Because the complement of  $\mathfrak{n}$  is a compact set it can be covered by a finite collection of open sets which are complements of ideals belonging to  $J$  in this case. Therefore  $\mathfrak{n}$  contains the intersection of finitely many elements of  $J$  so it must belong to this set by the above. Hence every  $\mathcal{O}$ -algebra homomorphism from  $R$  into an object of  $\mathcal{C}$  whose kernel contains  $\mathfrak{j}$  corresponds to an element of  $\text{Def}_S(A)$ . On the other hand let  $A$  be an object of  $\text{Ob}(\mathcal{C})$ , let  $D$  be an element of  $\text{Def}_S(A)$  and let  $f : R \rightarrow A$  the  $\mathcal{O}$ -algebra homomorphism corresponding to  $D$ . Then  $f$  is the composition of the quotient map  $\pi : R \rightarrow R/\mathfrak{n}$  for some open and closed ideal  $\mathfrak{n}$  and an injective homomorphism  $R/\mathfrak{n} \rightarrow A$ . By property (iii) above the element of  $\text{Def}'_S(R/\mathfrak{n})$  corresponding to  $\pi$  actually lies in  $\text{Def}_S(R/\mathfrak{n})$ . In particular the kernel  $\mathfrak{n}$  of the homomorphism  $f$  contains  $\mathfrak{j}$ . Hence the ring  $T = R/\mathfrak{j}$  pro-represents the functor  $\text{Def}_S(\cdot)$ .  $\square$

Let us return to the proof of Theorem 6.6. We are going to use the notation of Definition 6.3. Let  $G_S$  denote the Galois group of the maximal separable extension of  $F$  in  $\overline{F}$  which is unramified at every prime  $\mathfrak{q}$  not in  $S$ . For  $i = 0, 1, 2, 3$  let  $G_i$  and  $E_i$  denote the kernel of the canonical surjection  $p_i : GL_2(A_i) \rightarrow GL_2(\mathbb{F}_l)$  and the set

$$E_i = \{\rho : G_S \rightarrow GL_2(A_i) \mid p_i \circ \rho = \rho_l\},$$

respectively. Let moreover  $H_i$  denote the set of free  $A$ -submodules  $L \subset A^2$  of rank one which are direct summands of  $A^2$  and  $L \otimes_A \mathbb{F}_l = \overline{L}$ . The group  $G_i$  acts on  $E_i$  by conjugation and on  $H_i$  via its regular left action. Then

$$\text{Def}'_S(A_i) = (E_i \times H_i)/G_i \quad (i = 0, 1, 2, 3)$$

where we let  $G_i$  act diagonally on the product  $E_i \times H_i$ . For every pair  $\rho \times L \in E_i \times H_i$  let  $G_i(\rho \times L)$  denote the stabilizer of  $\rho \times L$  in  $G_i$ . For any  $\mathcal{C}$ -morphism  $f : A_i \rightarrow A_j$  for some  $i$  and  $j$  let  $D(f)$  denote the map  $D(f) : E_i \times H_i \rightarrow E_j \times H_j$  given by the rule  $D(f)(\rho \times L) = f \circ \rho \times L \otimes_{f(A_i)} A_j$ . Then the map  $h$  of Definition 6.3 is just the map

$$h : (E_i \times H_i)/G_i \rightarrow (E_i \times H_i)/G_i \times_{(E_i \times L_i)/G_i} (E_i \times H_i)/G_i$$

induced by  $D(\pi_1)$  and  $D(\pi_2)$ .

**Lemma 6.8.** *Assume that  $\phi_1$  is surjective. The following holds:*

- (i) *the map  $h$  is surjective,*
- (ii) *the map  $h$  is injective if the homomorphism  $G_1(\rho \times L) \rightarrow G_0(D(\phi_1)(\rho \times L))$  induced by  $\phi_1$  is surjective for every  $\rho \times L \in E_1 \times H_1$ .*

**Proof.** Let  $\rho_1 \times L_1 \in E_1 \times H_1$  and  $\rho_2 \times L_2 \in E_2 \times H_2$  be such that  $D(\phi_1)(\rho_1 \times L_1)$  and  $D(\phi_2)(\rho_2 \times L_2)$  lie in the same  $G_0$ -orbit. The homomorphism  $G_1 \rightarrow G_0$  induced by  $\phi_1$  is surjective hence there is a pair  $\rho'_1 \times L'_1 \in E_1 \times H_1$  in the  $G_1$ -orbit of  $\rho_1 \times L_1$  such that  $D(\phi_1)(\rho'_1 \times L'_1)$  is equal to  $D(\phi_2)(\rho_2 \times L_2)$ . Then there is a pair  $\rho_3 \times L_3 \in E_3 \times H_3$  such that  $D(\pi_1)(\rho_3 \times L_3) = \rho'_1 \times L'_1$  and  $D(\pi_2)(\rho_3 \times L_3) = \rho_2 \times L_2$  hence claim (i) is true. Now assume that the condition in claim (ii) holds and let  $\rho'_3 \times L'_3 \in E_3 \times H_3$  be another pair such that  $D(\pi_1)(\rho'_3 \times L'_3)$  lies in the  $G_1$ -orbit of  $\rho'_1 \times L'_1$  and  $D(\pi_2)(\rho'_3 \times L'_3)$  lies in the  $G_2$ -orbit of  $\rho_2 \times L_2$ . In order to prove that claim (ii) is true it will be enough to show that  $\rho_3 \times L_3$  and  $\rho'_3 \times L'_3$  are in the same  $G_3$ -orbit. Let  $g_1 \in G_1$  and  $g_2 \in G_2$  be two elements such that  $D(\pi_1)(\rho'_3 \times L'_3)g_1 = \rho'_1 \times L'_1$  and  $D(\pi_2)(\rho'_3 \times L'_3)g_2 = \rho_2 \times L_2$ . Let  $h_1$  and  $h_2$  denote the image of  $g_1$  under the natural map  $G_1 \rightarrow G_0$  and the image of  $g_2$  under the natural map  $G_2 \rightarrow G_0$ , respectively. Then  $h_2 h_1^{-1} \in G_0(D(\phi_1)(\rho'_1 \times L'_1))$  hence there is a  $g'_1 \in G_1(\rho'_1 \times L'_1)$  such that the image of  $g'_1$  maps to  $h_2 h_1^{-1}$  under the natural map  $G_1 \rightarrow G_0$ . The pair  $g'_1 g_1 \times g_2$  lies in the fiber product  $G_3 = G_1 \times_{G_0} G_2$  and maps  $\rho'_3 \times L'_3$  to  $\rho_3 \times L_3$ .  $\square$

With the aid of Lemma 6.8 the proof of Theorem 6.6 is now easy. Condition **H1** is immediate from claim (i) above. On the other hand conditions **H2** and **H4** follow at once from claim (ii) above and Lemma 6.9 below. We only need to prove now that  $\dim_{\mathbb{F}_l}(t_{\text{Def}'_S}(\cdot))$  is finite which is equivalent to the set  $\text{Def}'_S(\mathbb{F}_l[\epsilon])$  being finite. The set of affine lines  $L \subset \mathbb{F}_l[\epsilon]^2$  such that  $L \otimes_{\mathbb{F}_l[\epsilon]} \mathbb{F}_l = \overline{L}$  is obviously finite. On the hand the set

$$\{\rho : G_S \rightarrow GL_2(\mathbb{F}_l[\epsilon]) \mid a \circ \rho = \rho_l\}$$

is well-known to be bijective to the cohomology group  $H^1(G_S, \text{Ad}(\rho_l))$  which is finite.  $\square$

**Lemma 6.9.** *For every pair  $\rho \times L \in E_i \times H_i$  the stabilizer  $G_i(\rho \times L)$  is equal to  $G_i \cap Z(A_i)$  where  $Z(A_i)$  denotes the subgroup of scalar matrices in  $GL_2(A_i)$ .*

**Proof.** Let  $n$  denote the smallest natural number such that  $\mathfrak{m}_{A_i}^n \neq 0$  but  $\mathfrak{m}_{A_i}^{n+1} = 0$ . We are going to show that the stabilizer of  $\rho \times L$  in  $GL_2(A_i)$  is  $Z(A_i)$  by induction on  $n$ . When  $n = 0$  then  $A_i = \mathbb{F}_l$  and the claim above follows from a straightforward computation. Assume now that we know the claim for  $n - 1$  and let  $r$  be an element of the stabilizer of  $\rho \times L$ . By induction the image of  $r$  under the natural projection

$GL_2(A_i) \rightarrow GL_2(A_i/\mathfrak{m}_{A_i}^n)$  is a scalar matrix. Hence we may assume that  $r$  is actually the identity matrix under the image of this projection multiplying by a suitable scalar matrix. Now we only have to prove that  $r$  acts on  $(m_{A_i}^n)^2 \subset A_i^2$  as a scalar multiplication by an element of  $1 + \mathfrak{m}_{A_i}^n$ . But this is clear from the case  $n = 0$  as  $\rho|_{(m_{A_i}^n)^2} = \rho_l \otimes_{\mathbb{F}_l} (m_{A_i}^n)^2$  and  $L \cap (m_{A_i}^n)^2 = \overline{L} \otimes_{\mathbb{F}_l} (m_{A_i}^n)^2$ .  $\square$

## 7. HOMOMORPHISMS BETWEEN DEFORMATION RINGS AND HECKE RINGS

**Notation 7.1.** Let  $V = (M, \rho)$  be a representation of the topological group  $G$  over an object  $A$  of the category  $\mathcal{C}$  of Definition 6.2. For every  $\mathcal{C}$ -morphism  $f : A \rightarrow A'$  let  $V \otimes_A A'$  denote the couple  $(M \otimes_A A', \rho_{A'})$  where  $\rho_{A'}$  is the composition of  $\rho$  and the map  $GL_A(M) \rightarrow GL_{A'}(M \otimes_A A')$  which assigns  $\phi \otimes_A \text{id}_{A'}$  to  $\phi \in GL_A(M)$ . Recall that two representations  $(M, \rho)$  and  $(M', \rho')$  of  $G$  are said to be isomorphic if  $M$  and  $M'$  are isomorphic as  $A[G]$ -modules. When  $A$  is a field one may attach to every representation  $V = (M, \rho)$  another representation  $V_{ss} = (M_{ss}, \rho_{ss})$ , unique up to isomorphism, such that  $M_{ss}$  is semi-simple as an  $A[G]$ -module and has the same Jordan-Hölder components as the  $A[G]$ -module  $M$ . Let  $\mathbf{k}$  denote now a finite extension of  $\mathbb{F}_l$  and let  $V = (M, \rho)$  be a representation of  $\text{Gal}(\overline{F}|F)$  over  $\mathbf{k}$  which is unramified away from  $\mathfrak{p}$  and  $\infty$ , contains an affine  $\mathbf{k}$ -line  $L$  which is fixed by  $I_{\mathfrak{p}}$  but not left stable by  $\text{Gal}(\overline{F}|F)$  and the semi-simplification of  $V$  is isomorphic to the semi-simplification of  $(\mathbb{F}_l^2, \rho_l) \otimes_{\mathbb{F}_l} \mathbf{k}$ . Suppose moreover that the  $\mathbf{k}[D_{\infty}]$ -module  $M$  has a filtration:

$$0 \longrightarrow \mathbf{k}(1) \longrightarrow M \longrightarrow \mathbf{k} \longrightarrow 0$$

where  $\mathbf{k}(1)$ ,  $\mathbf{k}$  denotes the free  $\mathbf{k}$ -module of rank one equipped with the  $D_{\infty}$ -action given by  $\chi_{\mathbf{k}}|_{D_{\infty}}$  and the trivial character, respectively.

**Lemma 7.2.** *Under the assumptions above we have  $V \cong (\mathbb{F}_l, \rho_l) \otimes_{\mathbb{F}_l} \mathbf{k}$ .*

**Proof.** Because the Jordan-Hölder components of the  $\mathbf{k}[\text{Gal}(\overline{F}|F)]$ -modules corresponding to  $V$  and  $(\mathbb{F}_l, \rho_l) \otimes_{\mathbb{F}_l} \mathbf{k}$  are the same the  $\mathbf{k}[\text{Gal}(\overline{F}|F)]$ -module  $M$  is the extension of one of the  $\mathbf{k}[\text{Gal}(\overline{F}|F)]$ -modules given by the representations  $(\mathbb{F}_l, \overline{\chi}_l) \otimes_{\mathbb{F}_l} \mathbf{k}$  or  $(\mathbb{F}_l, 1) \otimes_{\mathbb{F}_l} \mathbf{k}$  by the other where 1 denotes the trivial representation. Because both  $\overline{\chi}_l$  and 1 are unramified at  $\mathfrak{p}$  the  $\mathbf{k}[\text{Gal}(\overline{F}|F)]$ -module  $M$  contains a non-zero submodule which is fixed by the inertia group  $I_{\mathfrak{p}}$ . On the other hand it also contains the affine line  $L$  which is fixed by  $I_{\mathfrak{p}}$  but not left stable by  $\text{Gal}(\overline{F}|F)$  hence as a  $\mathbf{k}$ -vectorspace  $M$  is spanned by vectors which is fixed by  $I_{\mathfrak{p}}$ . Therefore  $\rho$  is unramified at  $\mathfrak{p}$ . In a suitable basis the inertia group  $I_{\infty}$  acts by upper-triangular matrices which are equal to 1 on the diagonal. Therefore the representation  $\rho$  is tamely ramified at  $\infty$ . Because every étale cover of the affine line  $\mathbb{A}_{\mathbb{F}_q}^1$  which is tamely ramified at  $\infty$  is in fact unramified at  $\infty$  as well the Galois representation  $\rho$  is everywhere unramified. The only everywhere unramified extensions of  $F$  are the constant field extensions. As a representation of the absolute Galois group  $\text{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$ , where the latter group is isomorphic to the profinite completion of  $\mathbb{Z}$ , the representation  $(\mathbb{F}_l^2, \rho_l) \otimes_{\mathbb{F}_l} \mathbf{k}$  is the only one up to isomorphism which has an affine  $\mathbf{k}$ -line not fixed by the Galois action and has Jordan-Hölder components  $(\mathbb{F}_l, \overline{\chi}_l) \otimes_{\mathbb{F}_l} \mathbf{k}$  and  $(\mathbb{F}_l, 1) \otimes_{\mathbb{F}_l} \mathbf{k}$ .  $\square$

Let  $\text{Def}_{\min}(\cdot) : \mathcal{C} \rightarrow \text{Sets}$  denote the functor  $\text{Def}_S(\cdot)$  when  $S$  is the empty set. The functor  $\text{Def}_{\min}(\cdot)$  is called the minimal deformation problem.

**Proposition 7.3.** *The universal deformation ring of the minimal deformation problem  $\text{Def}_{\min}(\cdot)$  is  $\mathbb{Z}_l$ .*

**Proof.** We have to show that for every  $A \in \text{Ob}(\mathcal{C})$  the set  $\text{Def}_{\min}(A)$  has exactly one element because we have exactly one  $\mathbb{Z}_l$ -algebra homomorphism from  $\mathbb{Z}_l$  into  $A$ . First we are going to show that  $\text{Def}_{\min}(A)$  is not empty. Let  $\text{Fr}_\infty$  be again a lift of the Frobenius at the place  $\infty$  in  $\text{Gal}(\overline{F}|F)$ . Let  $\phi_l : \text{Gal}(\overline{F}|F) \rightarrow \mathbb{Z}_l$  be the unique map which factors through the Galois group of the maximal everywhere unramified extension of  $F$  such that  $\phi_l(\text{Fr}_\infty) = 1$  and  $\phi_l(gh) = \chi_l(h)\phi_l(g) + \phi_l(h)$  for every  $g, h \in \text{Gal}(\overline{F}|F)$ . Recall that  $\chi_A$  denotes the composition of the character  $\chi_l : \text{Gal}(\overline{F}|F) \rightarrow \mathbb{Z}_l^*$  and the natural map  $\mathbb{Z}_l^* \rightarrow A^*$ . Moreover let  $\phi_A$  be the composition of the twisted homomorphism  $\phi_l : \text{Gal}(\overline{F}|F) \rightarrow \mathbb{Z}_l$  and the natural map  $\mathbb{Z}_l \rightarrow A$ . Let  $\rho_A : \text{Gal}(\overline{F}|F) \rightarrow GL_2(A)$  denote the Galois representation such that

$$\rho_A(g) = \begin{pmatrix} 1 & 0 \\ 0 & \chi_A(g) \end{pmatrix} \quad (\forall g \in \text{Gal}(\overline{F}|F))$$

when  $l$  does not divide  $q - 1$  and

$$\rho_A(g) = \begin{pmatrix} 1 & \phi_A(g) \\ 0 & \chi_A(g) \end{pmatrix} \quad (\forall g \in \text{Gal}(\overline{F}|F))$$

when  $l$  does divide  $q - 1$ . Then for every  $A$ -module  $L \subset A^2$  of rank one such that  $L \otimes_A \mathbb{F}_l = \overline{L}$  the isomorphism class of the pair  $((A^2, \rho_A), L) \in \mathcal{P}_{\text{Gal}(\overline{F}|F)}(A)$  lies in  $\text{Def}_{\min}(A)$  as  $\rho_A$  is unramified at  $\mathfrak{p}$ . Let  $O = ((M, \rho), L)$  be now an arbitrary element of  $\text{Def}_{\min}(A)$ . By condition **D4** the inertia group  $I_\infty$  acts by upper-triangular matrices which are equal to 1 on the diagonal in a suitable  $A$ -basis of  $M$ . As the additive group of  $A$  is  $l$ -primary group the representation  $\rho$  is tamely ramified at  $\infty$ . Hence it must be everywhere unramified by the argument presented in the proof of Lemma 7.2 above. In particular the image of  $\rho$  is generated by  $\rho(\text{Fr}_\infty)$ . In any  $A$ -basis furnished by condition **D4** the matrix of  $\rho(\text{Fr}_\infty)$  is of the form:

$$\rho(\text{Fr}_\infty) = \begin{pmatrix} 1 & x \\ 0 & \chi_A(g) \end{pmatrix}$$

for some  $x \in A$ . Because the vector  $(0, 1)$  is fixed by  $\chi_A^{-1}\rho(\text{Fr}_\infty)$ , its reduction modulo  $\mathfrak{m}_A$  spans a one-dimensional subspace of  $M \otimes_A \mathbb{F}_l$  fixed by  $\chi_A^{-1}\rho \bmod \mathfrak{m}_A$ . But such a subspace is unique as  $\rho \bmod \mathfrak{m}_A$  is a conjugate of  $\overline{\rho}_l$ . Hence for a suitable  $y \in A^*$  the matrix of  $\rho(\text{Fr}_\infty) \bmod \mathfrak{m}_A$  in the basis  $(y, 0), (0, 1)$  is the same as the matrix of  $\rho_A(\text{Fr}_\infty)$ . Therefore there is a matrix  $m \in GL_2(A)$  such that  $m$  is congruent to the identity matrix  $\bmod \mathfrak{m}_A$  and  $m^{-1}\rho(\text{Fr}_\infty)m = \rho_A(\text{Fr}_\infty)$ . In other words we may assume that  $(M, \rho) = (A^2, \rho_A)$  and  $L \otimes_A \mathbb{F}_l = \overline{L}$ . Let  $H \subset GL_2(A)$  denote the subgroup:

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & y \end{pmatrix} \in GL_2(A) \mid y \equiv 1 \bmod \mathfrak{m}_A \right\}$$

when  $l$  does not divide  $q - 1$  and let  $H$  denote the subgroup:

$$H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 + (q-1)x \end{pmatrix} \in GL_2(A) \mid x \equiv 0 \bmod \mathfrak{m}_A \right\}$$

when  $l$  does divide  $q - 1$ . Then  $H$  commutes with  $\rho_A(\text{Fr}_\infty)$  and acts transitively on the set of affine lines  $L \subset A^2$  such that  $L \otimes_A \mathbb{F}_l = \overline{L}$ . Hence the set  $\text{Def}_{\min}(A)$  has at most one element.  $\square$



**Definition 7.4.** For every commutative ring  $A$  with unity and for every  $A$ -linear endomorphism  $m$  of a finitely generated free  $A$ -module let  $\text{Tr}(m) \in A$  denote the trace of  $m$ . Let  $\text{Def}_{\mathfrak{p}}(\cdot) : \mathcal{C} \rightarrow \text{Sets}$  denote the functor  $\text{Def}_S(\cdot)$  when  $S$  is the one-element set  $\{\mathfrak{p}\}$  and let  $R(\mathfrak{p})$  denote its universal deformation ring. The minimal deformation functor  $\text{Def}_{\min}(\cdot)$  is a sub-functor of  $\text{Def}_{\mathfrak{p}}(\cdot)$ . Let  $\pi_R : R(\mathfrak{p}) \rightarrow \mathbb{Z}_l$  be the surjective  $\mathbb{Z}_l$ -algebra homomorphism of universal deformation rings corresponding to this inclusion and let  $I_R \triangleleft R(\mathfrak{p})$  be the kernel of this projection. For every place  $v$  of  $F$  let  $\text{Fr}_v$  be a lift of the Frobenius at the place  $v$  in  $\text{Gal}(\overline{F}|F)$ . Let  $\mathfrak{n} \triangleleft R(\mathfrak{p})$  be an open and closed ideal and let  $((M, \rho), L) \in \mathcal{P}_{\text{Gal}(\overline{F}|F)}(R(\mathfrak{p})/\mathfrak{n})$  be a pair whose isomorphism class corresponds to the element of  $\text{Def}_{\mathfrak{p}}(R(\mathfrak{p})/\mathfrak{n})$  given by the canonical projection  $R(\mathfrak{p}) \rightarrow R(\mathfrak{p})/\mathfrak{n}$ . Then for every prime ideal  $\mathfrak{q} \neq \mathfrak{p}$  of  $\mathbf{A}$  the trace  $\text{Tr}(\rho(\text{Fr}_{\mathfrak{q}})) \in R(\mathfrak{p})/\mathfrak{n}$  is independent of choice of  $\text{Fr}_{\mathfrak{q}}$  as  $\rho$  is unramified at  $\mathfrak{q}$  (and of course it depends only on the isomorphism class of  $((M, \rho), L)$ ). The elements  $\text{Tr}(\rho(\text{Fr}_{\mathfrak{q}}))$  as  $\mathfrak{n}$  runs through the set of open and closed ideals of  $R(\mathfrak{p})$  form a compatible family and therefore has a limit in  $R(\mathfrak{p})$  which will be denoted by  $\text{Tr}(\rho_{\text{univ}}(\text{Fr}_{\mathfrak{q}}))$ .

**Proposition 7.5.** *The ideal  $I_R$  is generated by the set:*

$$\{1 + q^{\deg(\mathfrak{q})} - \text{Tr}(\rho_{\text{univ}}(\text{Fr}_{\mathfrak{q}})) | \mathfrak{p} \neq \mathfrak{q} \triangleleft \mathbf{A} \text{ is a prime ideal.}\}$$

**Proof.** (Compare with Proposition 3.3 of [1], pages 109-111.) Let  $J$  denote the ideal generated by the set in the claim above. Clearly  $J$  is a subset of  $I_R$  so we only have to show the other inclusion. Because  $R(\mathfrak{p})$  is a noetherian complete local ring the ideal  $J$  is the intersection of all open and closed ideals which contain  $J$ . Therefore it will be sufficient to prove that for every object  $A$  of  $\mathcal{C}$  and for every pair  $O = ((M, \rho), L)$  deforming  $O_l$  whose isomorphism class lies in  $\text{Def}_{\mathfrak{p}}(A)$  such that the image of  $J$  with respect to the  $\mathbb{Z}_l$ -homomorphism  $R(\mathfrak{p}) \rightarrow A$  corresponding to  $O$  is zero the Galois representation  $\rho$  is unramified at  $\mathfrak{p}$ . Assume first that  $l$  does not divide  $q - 1$ . By condition **D4** the module  $M$  has an  $A$ -basis such that the matrix of  $\rho(\text{Fr}_{\infty})$  is upper-triangular and the diagonal element of the first and second row is 1 and  $q$ , respectively. Conjugating by a suitable upper-triangular matrix we may even assume that  $\rho(\text{Fr}_{\infty})$  is of the form:

$$\rho(\text{Fr}_{\infty}) = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}.$$

If we write

$$\rho(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$$

for every  $g \in \text{Gal}(\overline{F}|F)$  in this basis then

$$a(g) = \frac{1}{q-1}(q\text{Tr}(\rho(g)) - \text{Tr}(\rho(\text{Fr}_{\infty}g)))$$

and

$$d(g) = \frac{1}{q-1}(\text{Tr}(\rho(\text{Fr}_{\infty}g)) - \text{Tr}(\rho(g))).$$

By assumption  $\text{Tr}(\text{Fr}_{\mathfrak{q}}) = 1 + \chi_A(\text{Fr}_{\mathfrak{q}})$  for every prime ideal  $\mathfrak{q} \neq \mathfrak{p}$  of  $\mathbf{A}$  hence  $\text{Tr}(h) = 1 + \chi_A(h)$  for every  $h \in \text{Gal}(\overline{F}|F)$  as well by the Chebotarev density

theorem. Therefore the equations above imply that  $a(g) = 1$  and  $d(g) = \chi_A(g)$  because  $\chi_A(\text{Fr}_\infty) = q$ . In particular for every  $g \in I_{\mathfrak{p}}$  we have:

$$\rho(g) = \begin{pmatrix} 1 & b(g) \\ c(g) & 1 \end{pmatrix}.$$

The affine line spanned by the vectors  $(1, 0)$  and  $(0, 1)$  modulo  $\mathfrak{m}_A$  are fixed by  $\rho(\text{Fr}_\infty) \bmod \mathfrak{m}_A$  hence by the action of the whole absolute Galois group as well. Hence the free  $A$ -module  $L \subset A^2$  of rank one is generated by a vector of the form  $(1, x)$  for some  $x \in A^*$ . Because

$$\rho(g)(1, x) = (1 + b(g)x, c(g) + x)$$

for every  $g \in I_{\mathfrak{p}}$  we must have  $b(g) = c(g) = 0$  in this case. In particular  $\rho$  is unramified at  $\mathfrak{p}$ . Assume now that  $l$  divides  $q - 1$ . Using condition **D4** as above we may conclude that the module  $M$  has an  $A$ -basis such that the matrix of  $\rho(\text{Fr}_\infty)$  is of the form:

$$\rho(\text{Fr}_\infty) = \begin{pmatrix} 1 & 1 \\ 0 & q \end{pmatrix}$$

in this basis. We may even assume that  $L$  is spanned by the vector  $(0, 1)$ . If we write

$$\rho(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$$

for every  $g \in \text{Gal}(\overline{F}|F)$  in this basis then

$$\text{Tr}(\rho(\text{Fr}_\infty g)) = a(g) + c(g) + qd(g) = 1 + q\chi_A(g)$$

using the same reasoning as above. Since every  $g \in I_{\mathfrak{p}}$  fixes  $(0, 1)$  we get that  $b(g) = 0$  and  $d(g) = 1$ . The determinant of  $\rho(g)$  is equal to  $\chi_A(g) = 1$  hence  $a(g) = 1$ . Therefore  $c(g) = 1 + q\chi_A(g) - (1 + q) = 0$  by the equation above. So  $\rho$  is unramified at  $\mathfrak{p}$  in this case as well.  $\square$

The following corollary follows from Proposition 7.5 above the same way as Corollary 3.4 of [1] on page 111 from Proposition 3.3 of the same paper.

**Corollary 7.6.** *The complete local  $\mathbb{Z}_l$ -algebra  $R(\mathfrak{p})$  is topologically generated by the elements  $\text{Tr}(\rho_{\text{univ}}(\text{Fr}_{\mathfrak{q}}))$  where  $\mathfrak{q} \neq \mathfrak{p}$  is any proper prime ideal of  $\mathbf{A}$ .  $\square$*

**Definition 7.7.** Let  $\widehat{\mathbb{T}}(\mathfrak{p})$  denote the commutative  $\mathbb{Z}$ -algebra with unity generated by the endomorphisms  $T_{\mathfrak{q}}$  of the  $\mathbb{Z}$ -module  $H(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$  where  $\mathfrak{q} \triangleleft \mathbf{A}$  is any prime ideal different from  $\mathfrak{p}$ . By Corollary 3.13 the algebra  $\widehat{\mathbb{T}}(\mathfrak{p})$  is a sub-algebra of the endomorphism ring of a finitely generated, free  $\mathbb{Z}$ -module hence it must be a finitely generated, free  $\mathbb{Z}$ -module, too. Let  $\widehat{\mathfrak{E}}(\mathfrak{p})$  denote the ideal of  $\widehat{\mathbb{T}}(\mathfrak{p})$  generated by the elements  $T_{\mathfrak{q}} - q^{\deg(\mathfrak{q})} - 1$ , where  $\mathfrak{q} \neq \mathfrak{p}$  is any prime. Because every generator  $T_{\mathfrak{q}}$  of  $\mathbb{T}_l(\mathfrak{p})$  is congruent to an element of  $\mathbb{Z}$  modulo the ideal  $\widehat{\mathfrak{E}}(\mathfrak{p})$  the natural inclusion of  $\mathbb{Z}$  in  $\widehat{\mathbb{T}}(\mathfrak{p})$  induces a surjection  $\mathbb{Z} \rightarrow \widehat{\mathbb{T}}(\mathfrak{p})/\widehat{\mathfrak{E}}(\mathfrak{p})$ . This map is also injective as the annihilator of the action of  $\widehat{\mathbb{T}}(\mathfrak{p})$  on the subgroup of  $H(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$  generated by  $E_{\mathfrak{p}}$  is equal to  $\widehat{\mathfrak{E}}(\mathfrak{p})$ . Therefore  $(l, \widehat{\mathfrak{E}}(\mathfrak{p}))$  is a maximal ideal in  $\widehat{\mathbb{T}}(\mathfrak{p})$  with residue field  $\mathbb{F}_l$ . Let  $T(\mathfrak{p})$  denote the completion of  $\widehat{\mathbb{T}}(\mathfrak{p})$  with respect to the maximal ideal  $(l, \widehat{\mathfrak{E}}(\mathfrak{p}))$  and for every prime ideal  $\mathfrak{q} \neq \mathfrak{p}$  of  $\mathbf{A}$  let  $T_{\mathfrak{q}} \in T(\mathfrak{p})$  denote the image of the Hecke operator  $T_{\mathfrak{q}}$  under the canonical projection  $\widehat{\mathbb{T}}(\mathfrak{p}) \rightarrow T(\mathfrak{p})$  by slight abuse of notation. The ring  $T(\mathfrak{p})$  is naturally equipped with the structure of a local  $\mathbb{Z}_l$ -algebra.

**Proposition 7.8.** *There is a unique  $\mathbb{Z}_l$ -algebra homomorphism  $\phi : R(\mathfrak{p}) \rightarrow T(\mathfrak{p})$  such that*

$$\phi(\mathrm{Tr}(\rho_{\mathrm{univ}}(\mathrm{Fr}_{\mathfrak{q}}))) = T_{\mathfrak{q}}$$

for every proper prime ideal  $\mathfrak{q} \neq \mathfrak{p}$  of  $\mathbf{A}$ .

**Proof.** Note that the map  $\phi$ , if it exists, is automatically surjective and local. So it is unique because it is determined on a set of topological generators by Corollary 7.6. Let  $\tilde{T}(\mathfrak{p})$  denote the normalization of the algebra  $T(\mathfrak{p})$  and let  $\iota : T(\mathfrak{p}) \rightarrow \tilde{T}(\mathfrak{p})$  be the normalization map. Because the  $T(\mathfrak{p})$  is a finitely generated free  $\mathbb{Z}_l$ -module the  $\mathbb{Z}_l$ -algebra  $\tilde{T}(\mathfrak{p})$  can be written as a finite product  $\prod_{i \in I} \mathcal{O}_i$  where each  $\mathcal{O}_i$  is a discrete valuation ring which is finitely generated and free as a  $\mathbb{Z}_l$ -module. For every  $i \in I$  let  $\pi_i : T(\mathfrak{p}) \rightarrow \mathcal{O}_i$  be the composition of  $\iota$  and the canonical projection. For every  $i \in I$  we are going to construct a  $\mathbb{Z}_l$ -algebra homomorphism  $\phi_i : R(\mathfrak{p}) \rightarrow \mathcal{O}_i$  such that

$$(7.8.1) \quad \phi_i(\mathrm{Tr}(\rho_{\mathrm{univ}}(\mathrm{Fr}_{\mathfrak{q}}))) = \pi_i(T_{\mathfrak{q}})$$

for every proper prime ideal  $\mathfrak{q} \neq \mathfrak{p}$  of  $\mathbf{A}$ . In this case the product

$$\phi = \prod_{i \in I} \phi_i : R(\mathfrak{p}) \rightarrow \prod_{i \in I} \mathcal{O}_i = \tilde{T}(\mathfrak{p})$$

maps  $R(\mathfrak{p})$  into the image of  $T(\mathfrak{p})$  with respect to  $\iota$  because  $\phi$  maps  $\mathrm{Tr}(\rho_{\mathrm{univ}}(\mathrm{Fr}_{\mathfrak{q}}))$  to  $\iota(T_{\mathfrak{q}})$  for every proper prime ideal  $\mathfrak{q} \neq \mathfrak{p}$  of  $\mathbf{A}$ . But  $\iota$  is injective hence the claim above implies the proposition.

Let  $\mathfrak{m}_i, \mathbf{k}_i$  denote the maximal ideal and the residue field of  $\mathcal{O}_i$ , respectively. Let  $\mathcal{O}'_i$  denote the preimage of  $\mathbb{F}_l \subseteq \mathbf{k}_i$  with respect to the residue map mod  $\mathfrak{m}_i$ . Then  $\mathcal{O}'_i/\mathfrak{m}_i = \mathbb{F}_l$  hence  $\mathcal{O}'_i/\mathfrak{m}_i^n$  is an object of the category  $\mathcal{C}$  for every positive integer  $n$ . Let  $\pi_{in} : GL_2(\mathcal{O}_i) \rightarrow GL_2(\mathcal{O}_i/\mathfrak{m}_i^n)$  denote the canonical projection. Note that it is sufficient to prove that there is a representation  $\rho_i : \mathrm{Gal}(\overline{F}|F) \rightarrow GL_2(\mathcal{O}_i)$  continuous with respect to the  $\mathfrak{m}_i$ -adic topology on  $GL_2(\mathcal{O}_i)$  and the Krull topology on  $\mathrm{Gal}(\overline{F}|F)$  along with a free  $\mathcal{O}_i$ -module  $L_i \subset \mathcal{O}_i^2$  of rank one satisfying the following properties:

- L1.** the order pair  $((\mathbb{F}_l^2, \pi_{i1} \circ \rho_i), L_i \otimes_{\mathcal{O}_i} \mathbb{F}_l)$  is isomorphic to  $\mathcal{O}_l \otimes_{\mathbb{F}_l} \mathbf{k}_i$ ,
- L2.** representation  $\rho_i$  is unramified at every prime ideal  $\mathfrak{q} \neq \mathfrak{p}$  of  $\mathbf{A}$ ,
- L3.** the inertia subgroup  $I_{\mathfrak{p}}$  at  $\mathfrak{p}$  acts trivially on the submodule  $L_i$ ,
- L4.** the determinant of  $\rho_i$  is equal to the composition  $\chi_i$  of the cyclotomic character  $\chi_l : \mathrm{Gal}(\overline{F}|F) \rightarrow \mathbb{Z}_l^*$  and the natural map  $\mathbb{Z}_l^* \rightarrow \mathcal{O}_i^*$ ,
- L5.** in a suitable  $\mathcal{O}_i$ -basis the matrix of  $\rho_i(g)$  for every  $g \in D_{\infty}$  is of the form:

$$\rho_i(g) = \begin{pmatrix} 1 & \psi_i(g) \\ 0 & \chi_i(g) \end{pmatrix}$$

for some  $\psi_i(g) \in \mathcal{O}_i$ ,

- L6.** we have  $\mathrm{Tr}(\rho_i(\mathrm{Fr}_{\mathfrak{q}})) = \pi_i(T_{\mathfrak{q}})$  for every prime ideal  $\mathfrak{q} \neq \mathfrak{p}$  of  $\mathbf{A}$ .

In fact when the claim above holds we may assume that the image of  $\rho_i$  lies in  $GL_2(\mathcal{O}'_i)$  and  $L_i = L'_i \otimes_{\mathcal{O}'_i} \mathcal{O}_i$  for some free  $\mathcal{O}'_i$ -module  $L'_i \subset (\mathcal{O}'_i)^2$  of rank one without loss of generality. In this case the isomorphism class of the pair  $((\mathcal{O}'_i/\mathfrak{m}_i)^2, \pi_{in} \circ \rho_i), L'_i \otimes_{\mathcal{O}'_i} \mathcal{O}'_i/\mathfrak{m}_i^n$  lies in  $\mathrm{Def}_{\mathfrak{p}}(\mathcal{O}'_i/\mathfrak{m}_i^n)$  for every positive integer  $n$ .

Let  $\phi_{in} : R(\mathfrak{p}) \rightarrow \mathcal{O}'_i/\mathfrak{m}_i^n$  denote the corresponding map. The maps  $\phi_{in}$  satisfy the obvious compatibility and their limit  $\phi : R(\mathfrak{p}) \rightarrow \mathcal{O}'_i$  satisfies the equation (7.8.1) above by condition **L6**.

In the rest of the proof we occupy ourselves with the proof of the existence of  $\rho_i$  and  $L_i$ . Assume first that the kernel of the projection  $\pi_i : T(\mathfrak{p}) \rightarrow \mathcal{O}_i$  contains the image of the ideal  $\widehat{\mathfrak{C}}(\mathfrak{p})$  with respect to the canonical projection  $\widehat{\mathbb{T}}(\mathfrak{p}) \rightarrow T(\mathfrak{p})$ . Then  $\mathcal{O}_i = \mathbb{Z}_l$  and  $\pi_i(T_{\mathfrak{q}}) = 1 + q^{\deg(\mathfrak{q})}$  for every prime ideal  $\mathfrak{q} \neq \mathfrak{p}$  of  $\mathbf{A}$ . Clearly the construction of Proposition 7.3 supplies the representation  $\rho_i$  in this case. Assume next that the kernel of the projection  $\pi_i : T(\mathfrak{p}) \rightarrow \mathcal{O}_i$  does not contain the image of the ideal  $\widehat{\mathfrak{C}}(\mathfrak{p})$  with respect to the canonical projection  $\widehat{\mathbb{T}}(\mathfrak{p}) \rightarrow T(\mathfrak{p})$ . Let  $j : \widehat{\mathbb{T}}(\mathfrak{p}) \rightarrow \mathbb{T}(\mathfrak{p}) \oplus \mathbb{Z}$  denote the direct sum of the surjections  $j_1 : \widehat{\mathbb{T}}(\mathfrak{p}) \rightarrow \mathbb{T}(\mathfrak{p})$  and  $j_2 : \widehat{\mathbb{T}}(\mathfrak{p}) \rightarrow \mathbb{Z}$  induced by the restriction of the action of  $\widehat{\mathbb{T}}(\mathfrak{p})$  onto  $H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$  and  $\mathbb{Z}E_{\mathfrak{p}}$ , respectively. By Theorem 3.12 and its Corollary 3.13 the direct sum  $H_1(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})} \oplus \mathbb{Z}E_{\mathfrak{p}}$  is a subgroup of finite index of  $H(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{p})}$ . Hence  $j \otimes \mathbb{Q} : \widehat{\mathbb{T}}(\mathfrak{p}) \otimes \mathbb{Q} \rightarrow \mathbb{T}(\mathfrak{p}) \otimes \mathbb{Q} \oplus \mathbb{Q}$  is an isomorphism. Therefore the composition  $\pi'_i$  of the canonical surjection  $\widehat{\mathbb{T}}(\mathfrak{p}) \rightarrow T(\mathfrak{p})$  and  $\pi_i$  factors through  $j_1$ .

The image  $R$  of  $\pi'_i$  is an order in a number field  $K$ . The image of the ideal  $(\widehat{\mathfrak{C}}(\mathfrak{n}), l)$  with respect to  $\pi'_i$  is a maximal ideal  $\mathfrak{m}$  in  $R$  such that  $R/\mathfrak{m} = \mathbb{F}_l$ . Let  $K_i$  denote the completion of  $K$  with respect to the valuation corresponding to the ideal  $\mathfrak{m}$ . The valuation ring of  $K_i$  is obviously  $\mathcal{O}_i$ . Let  $A$  be an abelian variety over  $F$  equipped with  $R$ -multiplication whose existence is guaranteed by Theorem 4.8. The  $R$ -multiplication on  $A$  induces a  $K_i$ -linear structure on  $V_l(A)$  which makes the latter a  $K_i$ -vectorspace of dimension two. Let  $W$  denote this vector space. The action of the absolute Galois group of  $F$  on  $V_l(A)$  is  $K_i$ -linear hence it induces a homomorphism  $\rho'_i : \text{Gal}(\overline{F}|F) \rightarrow GL_{K_i}(W)$ . Because the topological group  $\text{Gal}(\overline{F}|F)$  is compact and the representation is continuous with respect to the topology of  $W$  induced by the valuation of  $K_i$  there is a free  $\mathcal{O}_i$ -submodule  $V \subset W$  of rank two left stable by  $\text{Gal}(\overline{F}|F)$ . Because  $A$  has semi-stable reduction at  $\mathfrak{p}$  there is a unique 1-dimensional  $K_i$ -subspace  $U$  of  $W$  fixed by  $I_{\mathfrak{p}}$ . Let  $L$  denote the intersection of  $V$  and  $U$  and fix an  $\mathcal{O}_i$ -linear isomorphism  $c : \mathcal{O}_i^2 \rightarrow V$ . Such an isomorphism furnishes a homomorphism  $\rho_i : \text{Gal}(\overline{F}|F) \rightarrow GL_2(\mathcal{O}_i)$  by restricting the action of  $\text{Gal}(\overline{F}|F)$  via  $\rho'_i$  onto  $V$ . We claim that  $\rho_i$  along with  $L_i = c^{-1}(L)$  satisfy **L1-L6** for a suitable choice of  $V$ .

In any case  $\rho_i$  satisfies condition **L2** because  $A$  has good reduction at every prime ideal  $\mathfrak{q} \neq \mathfrak{p}$  of  $\mathbf{A}$ . Condition **L3** is obvious and **L4** is consequence of the fact that  $\rho_i$  comes from the Tate-module of an abelian variety. Similarly **L5** and **L6** are automatic as  $A$  has split multiplicative reduction at  $\infty$  and by condition (iii) of Theorem 4.8, respectively. Let  $u \in \mathcal{O}_i$  be a uniformizer. Note that

$$\text{Tr}(\rho_i(\text{Fr}_{\mathfrak{q}})) = \pi_i(T_{\mathfrak{q}}) \equiv 1 + q^{\deg(\mathfrak{q})} \pmod{\mathfrak{m}_i}$$

for every prime ideal  $\mathfrak{q} \neq \mathfrak{p}$  of  $\mathbf{A}$ . So the eigenvalues of  $\pi_{i1} \circ \rho_i(\text{Fr}_{\mathfrak{q}})$  are 1 and  $\chi_l(\text{Fr}_{\mathfrak{q}})$  therefore the semisimplification of  $(\mathbf{k}_i^2, \pi_{i1} \circ \rho_i)$  is isomorphic to the semisimplification of  $(\mathbb{F}_l^2, \rho_l) \otimes_{\mathbb{F}_l} \mathbf{k}_i$  by the Chebotarev density theorem. Hence the pair  $(\rho_i, L_i)$  will also satisfy **L1** if the image of  $L$  in  $V/uV$  is not left invariant by  $\text{Gal}(\overline{F}|F)$  according to Lemma 7.2. Because  $W$  is irreducible as a  $\text{Gal}(\overline{F}|F)$ -module the  $\mathcal{O}_i$ -module  $L$  is not left stable by  $\text{Gal}(\overline{F}|F)$ . Hence there is a positive integer  $n > 0$  such that the image of  $L$  under the action of  $\text{Gal}(\overline{F}|F)$  does not lie in  $u^n V + L$ . Let

$n$  denote actually the smallest such number and let  $V'$  denote the  $\mathcal{O}_i$ -submodule  $u^{n-1}V + L$ . Then  $V'$  is left invariant by  $\text{Gal}(\overline{F}|F)$  and the image of  $L \subset V'$  in  $V'/uV'$  is not left invariant by  $\text{Gal}(\overline{F}|F)$ .  $\square$

## 8. CALCULATIONS WITH INFINITESIMAL DEFORMATIONS

**Definition 8.1.** In this chapter every sheaf or cohomology group is understood to be over the étale site. Let  $U$  denote the affine curve  $\mathbb{P}_{\mathbb{F}_q}^1 - \{\mathfrak{p}, \infty\}$  over  $\mathbb{F}_q$ . Let  $\overline{S}$  denote the base change of  $S$  to  $\text{Spec}(\mathbb{F}_q)$  for every  $\text{Spec}(\mathbb{F}_q)$ -scheme  $S$ . Fix a  $\mathbb{F}_q$ -valued point  $v$  of  $\overline{U}$ . Then there is an exact sequence:

$$0 \longrightarrow \pi_1^{et}(\overline{U}, v) \longrightarrow \pi_1^{et}(U, v) \longrightarrow \text{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q) \longrightarrow 0$$

of profinite groups. The absolute Galois group  $\text{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$  is isomorphic to the profinite completion  $\widehat{\mathbb{Z}}$  of  $\mathbb{Z}$  and it is equipped with a natural topological generator  $\sigma \in \text{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$ , the arithmetic Frobenius. Let  $\mathbf{K}_l \triangleleft \pi_1^{et}(\overline{U}, v)$  denote the intersection of the kernels of all surjective homomorphisms  $s : \pi_1^{et}(\overline{U}, v) \rightarrow M$  where  $M$  is a finite abelian group of  $l$ -power order. Then  $\mathbf{K}_l$  is a characteristic subgroup of  $\pi_1^{et}(\overline{U}, v)$  hence it is a normal subgroup of  $\pi_1^{et}(U, v)$ . Let  $\mathbf{G}_l$  denote the quotient  $\pi_1^{et}(U, v)/\mathbf{K}_l$ .

**Lemma 8.2.** *The following holds:*

- (i) *the group  $\mathbf{G}_l$  is isomorphic to a semidirect product  $\mathbf{H}_l \rtimes \text{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$  where  $\mathbf{H}_l$  is a finitely generated and free  $\mathbb{Z}_l$ -module,*
- (ii) *the module  $\mathbf{H}_l$  has a  $\mathbb{Z}_l$ -basis  $e_1, e_2, \dots, e_{\deg(\mathfrak{p})}$  such that the action of  $\sigma$  on  $\mathbf{H}_l$  induced by conjugation is given by the rule  $\sigma(e_{\deg(\mathfrak{p})}) = qe_1$  and  $\sigma(e_n) = qe_{n+1}$  when  $n < \deg(\mathfrak{p})$ .*

**Proof.** Let  $\mathbf{H}_l$  and  $t$  denote the image of  $\pi_1^{et}(\overline{U}, v)$  and the image of the Frobenius  $\text{Fr}_\infty$  in  $\mathbf{G}_l$  with respect to the quotient map  $\pi_1^{et}(U, v) \rightarrow \mathbf{G}_l$ , respectively. Then  $\mathbf{H}_l$  is a normal subgroup of  $\mathbf{G}_l$  and  $t \in \mathbf{G}_l$  is an element whose image with respect to the canonical surjection  $\mathbf{G}_l \rightarrow \text{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$  is  $\sigma$ . Hence the subgroup  $\langle t \rangle$  of  $\mathbf{G}_l$  generated topologically by  $t$  is isomorphic to  $\text{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$  and  $\mathbf{G}_l$  is the semidirect product  $\mathbf{H}_l \rtimes \langle t \rangle$ . By definition  $\mathbf{H}_l$  is the maximal pro- $l$  abelian quotient of  $\pi_1^{et}(\overline{U}, v)$  hence it is a free, finitely generated  $\mathbb{Z}_l$ -module isomorphic to  $\text{Hom}_{\mathbb{Z}_l}(H^1(\overline{U}, \mathbb{Z}_l), \mathbb{Z}_l)$ . Consider the long cohomological exact sequence:

$$H^0(\overline{U}, \mathcal{O}^*) \xrightarrow{l^n} H^0(\overline{U}, \mathcal{O}^*) \xrightarrow{\delta_n} H^1(\overline{U}, \mu_{l^n}) \longrightarrow H^1(\overline{U}, \mathcal{O}^*)$$

attached to the Kummer exact sequence:

$$0 \longrightarrow \mu_{l^n} \longrightarrow \mathcal{O}^* \xrightarrow{l^n} \mathcal{O}^* \longrightarrow 0$$

where  $\mu_{l^n}$  denotes the sheaf of  $l^n$ -th roots of unity as usual. The group  $H^1(\overline{U}, \mathcal{O}^*)$  is isomorphic to the Picard group of  $\overline{U}$  but the latter is zero because  $\overline{U}$  is the spectrum of a unique factorization domain. Hence the coboundary maps  $\delta_n$  are surjective and their limit induce an isomorphism:

$$\delta : H^1(\overline{U}, \mathcal{O}^*) \otimes \mathbb{Z}_l \cong H^1(U, \mathbb{Z}_l(1)).$$

Let  $\Delta$  denote the set of closed points of the projective line over  $\overline{\mathbb{F}}_q$  in the complement of  $\overline{U}$  which are different from  $\infty$ . Let  $\mathbb{Z}_l[\Delta]$  denote the  $\mathbb{Z}_l$ -module generated freely by the elements of  $\Delta$ . The natural  $\text{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ -action on  $\Delta$  induces a  $\text{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ -module structure on  $\mathbb{Z}_l[\Delta]$ . The valuation maps at the elements of  $\Delta$  induce a  $\text{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ -module isomorphism:

$$j_0 : H^0(\overline{U}, \mathcal{O}^*) \otimes \mathbb{Z}_l \cong \mathbb{Z}_l[\Delta].$$

Because  $\mathfrak{p}$  is a prime ideal the set  $\Delta$  can be indexed by the natural numbers  $n = 1, 2, \dots, \deg(\mathfrak{p})$  such that  $\sigma(n) = n + 1$  when  $n < \deg(\mathfrak{p})$  and  $\sigma(\deg(\mathfrak{p})) = 1$ . Therefore the group:

$$\mathbf{H}_l \cong \text{Hom}_{\mathbb{Z}_l}(H^1(\overline{U}, \mathbb{Z}_l), \mathbb{Z}_l) = \text{Hom}_{\mathbb{Z}_l}(H^1(\overline{U}, \mathbb{Z}_l(1)) \otimes_{\mathbb{Z}_l} \mathbb{Z}_l(-1), \mathbb{Z}_l)$$

satisfies the properties in claims (i) and (ii).  $\square$

**Definition 8.3.** Any  $\mathbb{Z}_l$ -basis  $e_1, e_2, \dots, e_{\deg(\mathfrak{p})}$  of  $\mathbf{H}_l$  where the action of  $\sigma$  is given by the rule in part (ii) will be called a  $\sigma$ -cyclic basis. By slight abuse of notation let  $\text{Fr}_x$  denote the image of the Frobenius  $\text{Fr}_x$  in  $\mathbf{G}_l$  with respect to the quotient map  $\pi_1^{et}(U, v) \rightarrow \mathbf{G}_l$  for every place  $x$  of  $F$ . The image of the inertia group  $I_x$  with respect to the quotient map  $\pi_1^{et}(U, v) \rightarrow \mathbf{G}_l$  lies in  $\mathbf{H}_l$  hence the induced map  $I_x \rightarrow \mathbf{H}_l$  factors through the largest pro- $l$  quotient  $I_{x,l}$  of  $I_x$ . The group  $I_{x,l}$  is isomorphic to  $\mathbb{Z}_l$  and it has a topological generator  $i_x$  such that under the action of  $\text{Fr}_x$  on  $I_{x,l}$  induced by conjugation the element  $i_x$  maps to  $q^{\deg(x)}i_x$ . By the usual abuse of notation let  $i_x$  denote the image of the element  $i_x$  in  $\mathbf{H}_l$  as well with respect to the map  $I_{x,l} \rightarrow \mathbf{H}_l$  induced by the quotient map  $\pi_1^{et}(U, v) \rightarrow \mathbf{G}_l$  for every place  $x$  of  $F$ .

**Lemma 8.4.** *There is a  $\sigma$ -cyclic basis  $e_1, e_2, \dots, e_{\deg(\mathfrak{p})}$  of  $\mathbf{H}_l$  such that  $i_{\mathfrak{p}} = e_1$  and  $i_{\infty} = u \sum_{n=1}^{\deg(\mathfrak{p})} e_n$  for some  $u \in \mathbb{Z}_l^*$ .*

**Proof.** The image of  $\text{Fr}_{\mathfrak{p}}$  with respect to the quotient map  $\mathbf{G}_l \rightarrow \text{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$  is  $\sigma^{\deg(\mathfrak{p})}$ . Hence  $\sigma^{\deg(\mathfrak{p})}(i_{\mathfrak{p}}) = q^{\deg(\mathfrak{p})}i_{\mathfrak{p}}$  under the action induced by conjugation. Let  $B_l \triangleleft \mathbf{G}_l$  denote the closed normal subgroup generated by  $i_{\mathfrak{p}}$ . Then  $B_l$  is a subgroup of  $\mathbf{H}_l$  and as a  $\mathbb{Z}_l$ -module it is generated by the elements  $e_n = q^{1-n}\sigma^{n-1}(i_{\mathfrak{p}})$  where  $n = 1, 2, \dots, \deg(\mathfrak{p})$ . The quotient  $\mathbf{G}_l/B_l$  is a Galois group which is unramified at  $\mathfrak{p}$  and tamely ramified at  $\infty$  hence it is everywhere unramified. Therefore  $B_l = \mathbf{H}_l$  and  $e_1, e_2, \dots, e_{\deg(\mathfrak{p})}$  is a  $\sigma$ -cyclic basis. The image of  $\text{Fr}_{\infty}$  with respect to the quotient map  $\mathbf{G}_l \rightarrow \text{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$  is  $\sigma$  hence  $\sigma(i_{\infty}) = qi_{\infty}$  under the action induced by conjugation. Therefore  $i_{\infty}$  lies in the  $\mathbb{Z}_l$ -module generated by the element  $\sum_{n=1}^{\deg(\mathfrak{p})} e_n$ . The quotient of  $\mathbf{H}_l$  by the  $\mathbb{Z}_l$ -module generated by  $i_{\infty}$  is isomorphic to  $\pi_1^{et}(\overline{S}, v) = \text{Hom}_{\mathbb{Z}_l}(H^1(\overline{S}, \mathbb{Z}_l), \mathbb{Z}_l)$  where  $S$  is the complement of  $\mathfrak{p}$  in the projective line. The group  $H^1(\overline{S}, \mathbb{Z}_l)$  is torsion-free so  $i_{\infty} = u \sum_{n=1}^{\deg(\mathfrak{p})} e_n$  for some  $u \in \mathbb{Z}_l^*$ .  $\square$

**Definition 8.5.** Let  $\text{Def}_{\mathfrak{p}}^0(A[\epsilon]) \subseteq \text{Def}_{\mathfrak{p}}(A[\epsilon])$  denote the pre-image of the unique element of  $\text{Def}_{\min}(A)$  with respect to the map  $\text{Def}_{\mathfrak{p}}(A[\epsilon]) \rightarrow \text{Def}_{\mathfrak{p}}(A)$  induced by the augmentation homomorphism  $a : A[\epsilon] \rightarrow A$ . We say that an ordered pair  $((A[\epsilon]^2, \rho), L)$  representing an element of  $\text{Def}_{\mathfrak{p}}^0(A[\epsilon])$  is in standard form if the following holds:

- S1.** the  $A[\epsilon]$ -module  $L$  is generated by  $(1, 1)$ , when  $l$  does not divide  $q - 1$  and it is generated by  $(0, 1)$ , otherwise,

**S2.** the matrix of  $\rho(g)$  for every  $g \in D_\infty$  is of the form:

$$\rho(g) = \begin{pmatrix} 1 & \psi(g) \\ 0 & \chi_{A[\epsilon]}(g) \end{pmatrix}$$

for some  $\psi(g) \in A[\epsilon]$  such that  $\psi(\text{Fr}_\infty) = 0$ , when  $l$  does not divide  $q - 1$  and  $\psi(\text{Fr}_\infty) = 1$ , otherwise.

Because there is no ambiguity in this case we will simply let  $\rho$  denote this ordered pair. In order to avoid the use of awkward terminology we will call such an object  $\rho$  a representation in standard form. The argument of Proposition 7.5 shows that every element of  $\text{Def}_p^0(A[\epsilon])$  can be represented by a representation  $\rho$  in standard form. Note that the image of  $\pi_1^{\text{et}}(\overline{U}, v)$  under  $\rho$  is a finite abelian group of  $l$ -power order. Hence  $\rho$  factors through  $\mathbf{G}_l$ . Let  $\rho : \mathbf{G}_l \rightarrow GL_2(A[\epsilon])$  denote the corresponding homomorphism as well by slight abuse of notation.

**Lemma 8.6.** *Assume that  $\rho$  is in standard form. Then*

$$\rho(i_p) = \begin{cases} \begin{pmatrix} 1 + a(\rho)\epsilon & -a(\rho)\epsilon \\ a(\rho)\epsilon & 1 - a(\rho)\epsilon \end{pmatrix}, & \text{if } l \nmid q - 1, \\ \begin{pmatrix} 1 & 0 \\ a(\rho)\epsilon & 1 \end{pmatrix}, & \text{otherwise.} \end{cases}$$

for some  $a(\rho) \in A$ .

**Proof.** Let  $\pi : GL_2(A[\epsilon]) \rightarrow GL_2(A)$  denote the homomorphism induced by the augmentation map  $a : A[\epsilon] \rightarrow A$ . Because  $\pi \circ \rho(i_p)$  is the identity matrix we have:

$$\rho(i_p) = \begin{pmatrix} 1 + a\epsilon & b\epsilon \\ c\epsilon & 1 + d\epsilon \end{pmatrix}$$

for some  $a, b, c, d \in A$ . The determinant of  $\rho(i_p)$  is trivial hence  $a + d = 0$ . When  $l$  does not divide  $q - 1$  the matrix  $\rho(i_p)$  fixes the vector  $(1, 1)$  hence  $a + b = c + d = 0$ . When  $l$  does divide  $q - 1$  the matrix  $\rho(i_p)$  fixes the vector  $(0, 1)$  hence  $b = d = 0$ . The claim is now clear.  $\square$

Let  $l(\mathfrak{p})$  denote the largest power of  $l$  dividing  $N(\mathfrak{p})$ .

**Proposition 8.7.** *Assume that  $\rho$  is in standard form. Using the notation of the lemma above we have  $l(\mathfrak{p})a(\rho) = 0$ .*

**Proof.** For the sake of simple notation let  $d$  denote  $\deg(\mathfrak{p})$ . Assume first that  $l$  does not divide  $q - 1$ . Then

$$\begin{aligned} \begin{pmatrix} 1 + q^d a(\rho)\epsilon & -q^d a(\rho)\epsilon \\ q^d a(\rho)\epsilon & 1 - q^d a(\rho)\epsilon \end{pmatrix} &= \rho(i_p)^{q^d} = \rho(\text{Fr}_\infty)^{-d} \rho(i_p) \rho(\text{Fr}_\infty)^d \\ &= \begin{pmatrix} 1 + a(\rho)\epsilon & -q^d a(\rho)\epsilon \\ q^{-d} a(\rho)\epsilon & 1 - a(\rho)\epsilon \end{pmatrix} \end{aligned}$$

by Lemma 8.4 hence  $(q^d - 1)a(\rho) = 0$ . On the other hand  $\prod_{n=0}^{d-1} (\text{Fr}_\infty^{-n} i_p \text{Fr}_\infty^n)^{q^{-n}}$  lies in the image of the inertia group  $I_\infty$  in  $\mathbf{G}_l$  by Lemma 8.4 hence the matrix:

$$\begin{aligned} \prod_{n=0}^{d-1} (\rho(\text{Fr}_\infty)^{-n} \rho(i_p) \rho(\text{Fr}_\infty)^n)^{q^{-n}} &= \prod_{n=0}^{d-1} \begin{pmatrix} 1 + a(\rho)\epsilon & -q^n a(\rho)\epsilon \\ q^{-n} a(\rho)\epsilon & 1 - a(\rho)\epsilon \end{pmatrix}^{q^{-n}} \\ &= \begin{pmatrix} 1 + \sum_{n=0}^{d-1} q^{-n} a(\rho)\epsilon & -da(\rho)\epsilon \\ \sum_{n=0}^{d-1} q^{-2n} a(\rho)\epsilon & 1 - \sum_{n=0}^{d-1} q^{-n} a(\rho)\epsilon \end{pmatrix} \end{aligned}$$

is upper-triangular with ones on the diagonal. Hence  $(q^d - 1)/(q - 1)$  and  $(q^{2d} - 1)/(q^2 - 1)$  annihilates  $a(\rho)$ , too. The greatest common divisor of these numbers is:

$$\left( \frac{q^d - 1}{q - 1}, \frac{q^{2d} - 1}{q^2 - 1} \right) = N(\mathfrak{p}) \cdot \begin{cases} (1, \frac{q^d + 1}{q + 1}), & \text{if } d \text{ is odd,} \\ (q + 1, q^d + 1), & \text{otherwise.} \end{cases}$$

In any case the greatest common divisor on the right hand side of the equation above divides 2. Because  $l$  does not divide  $q - 1$  it is odd so the claim above holds in this case. Assume now that  $l$  does divide  $q - 1$ . Then

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ q^d a(\rho)\epsilon & 1 \end{pmatrix} &= \rho(i_{\mathfrak{p}})^{q^d} = \rho(\text{Fr}_{\infty})^{-d} \rho(i_{\mathfrak{p}}) \rho(\text{Fr}_{\infty})^d \\ &= \begin{pmatrix} 1 + \frac{q^{-d}-1}{q-1} a(\sigma)\epsilon & \frac{(q^{-d}-1)(q^d-1)}{(q-1)^2} a(\sigma)\epsilon \\ q^{-d} a(\rho)\epsilon & 1 - \frac{q^{-d}-1}{q-1} a(\sigma)\epsilon \end{pmatrix} \end{aligned}$$

hence  $(q^d - 1)/(q - 1)$  annihilates  $a(\rho)$ . As we saw above the matrix:

$$\begin{aligned} \prod_{n=0}^{d-1} \rho(\text{Fr}_{\infty}^{-n} i_{\mathfrak{p}} \text{Fr}_{\infty}^n)^{q^{-n}} &= \prod_{n=0}^{d-1} \begin{pmatrix} 1 + \frac{q^{-n}-1}{q-1} a(\sigma)\epsilon & \frac{(q^{-n}-1)(q^n-1)}{(q-1)^2} a(\sigma)\epsilon \\ q^{-n} a(\rho)\epsilon & 1 - \frac{q^{-n}-1}{q-1} a(\sigma)\epsilon \end{pmatrix}^{q^{-n}} \\ &= \begin{pmatrix} 1 + \sum_{n=0}^{d-1} q^{-n} \frac{q^{-n}-1}{q-1} a(\rho)\epsilon & - \sum_{n=0}^{d-1} \left( \frac{q^{-n}-1}{q-1} \right)^2 a(\rho)\epsilon \\ \sum_{n=0}^{d-1} q^{-2n} a(\rho)\epsilon & 1 - \sum_{n=0}^{d-1} q^{-n} \frac{q^{-n}-1}{q-1} a(\rho)\epsilon \end{pmatrix} \end{aligned}$$

is upper-triangular with ones on the diagonal hence  $(q^{2d} - 1)/(q^2 - 1)$  annihilates  $a(\rho)$  in this case, too. So the claim holds unless  $d$  and  $l$  are even. In the latter case we also need to use that the number:

$$q^{2d-2} \left( \sum_{n=0}^{d-1} q^{-n} \frac{q^{-n}-1}{q-1} \right) = \frac{1}{q-1} \left( \frac{q^{2d}-1}{q^2-1} - q^{d-1} \frac{q^d-1}{q-1} \right) = -\frac{q^d-1}{q^2-1} \cdot \frac{q^{d-1}-1}{q-1}$$

annihilates  $a(\rho)$ . Since

$$\frac{q^{d-1}-1}{q-1} = q^{d-2} + \dots + 1 \equiv d-1 \equiv 1 \pmod{2}$$

in this case, the claim holds when  $l = 2$  and  $d$  is even as well.  $\square$

**Proposition 8.8.** *The group  $I_R/I_R^2$  is cyclic and its order divides  $l(\mathfrak{p})$ .*

**Proof.** It will be sufficient to prove the same about the group  $(I_R, l^n)/(I_R^2, l^n)$  for every positive integer  $n$ . Because  $(I_R, l^n)/(I_R^2, l^n)$  is finite and annihilated by  $l^n$  it will be sufficient to prove the same about the group  $\text{Hom}((I_R, l^n)/(I_R^2, l^n), \mathbb{Z}/(l^n))$ . Let  $A$  be an object of  $\mathcal{C}$ . We say that a  $\mathbb{Z}_l$ -homomorphism  $\psi : R(\mathfrak{p}) \rightarrow A[\epsilon]$  is  $I_R$ -admissible if  $\psi(I_R)$  lies in the ideal of  $A[\epsilon]$  generated by  $\epsilon$ . Note that a  $\mathbb{Z}_l$ -homomorphism  $\psi : R(\mathfrak{p}) \rightarrow A[\epsilon]$  is  $I_R$ -admissible if and only if the element of  $\text{Def}_{\mathfrak{p}}(A[\epsilon])$  corresponding to  $\psi$  lies in  $\text{Def}_{\mathfrak{p}}^0(A[\epsilon])$ . For every  $I_R$ -admissible  $\mathbb{Z}_l$ -homomorphism  $\psi : R(\mathfrak{p}) \rightarrow \mathbb{Z}/(l^n)[\epsilon]$  let  $T(\psi) : (I_R, l^n) \rightarrow \mathbb{Z}/(l^n)$  denote the unique  $\mathbb{Z}_l$ -linear map such that  $\psi(i) = T(\psi)(i)\epsilon$  for every  $i \in (I_R, l^n)$ . The homomorphism



$T(\psi)$  factors through  $(I_R^2, l^n)$  and the map given by the rule  $\psi \mapsto T(\psi)$  induces a bijection  $b_n$  between the set  $\text{Adm}(\mathbb{Z}/(l^n))$  of  $I_R$ -admissible  $\mathbb{Z}_l$ -homomorphisms  $\psi : R(\mathfrak{p}) \rightarrow \mathbb{Z}/(l^n)[\epsilon]$  and the set  $\text{Hom}((I_R, l^n)/(I_R^2, l^n), \mathbb{Z}/(l^n))$ . Under this bijection the set  $\text{Adm}(\mathbb{Z}/(l^n))$  is equipped with a group structure.

Let  $\rho_1$  and  $\rho_2$  be two representations in standard form representing two elements of the set  $\text{Def}_{\mathfrak{p}}^0(\mathbb{Z}/(l^n)[\epsilon])$ . We define the sum  $\rho_3$  of  $\rho_1$  and  $\rho_2$  as the unique representation in standard form such that the latter, as a representation of  $\text{Gal}(\overline{F}|F)$  on  $\mathbb{Z}/(l^n)[\epsilon]^2$ , is given by the rule:

$$\rho_3(g) = \rho_1(g) + \rho_2(g) - \rho_0(g), \quad \forall g \in \text{Gal}(\overline{F}|F),$$

where  $\rho_0$  is the representation  $\rho_{A[\epsilon]}$  constructed in the proof of Lemma 7.3. It is very easy to see that this operation makes the set of representations in standard form into a group  $\text{St}(\mathbb{Z}/(l^n))$  with  $\rho_0$  as the zero element. Let  $\psi_i$  be the element of  $\text{Adm}(\mathbb{Z}/(l^n))$  corresponding to  $\rho_i$  where  $i = 1, 2, 3$ . Then  $\psi_3$  is the sum of  $\psi_1$  and  $\psi_2$ . Hence  $\text{Hom}((I_R, l^n)/(I_R^2, l^n), \mathbb{Z}/(l^n))$  is the quotient of  $\text{St}(\mathbb{Z}/(l^n))$ . Let  $\rho$  be an element of  $\text{St}(\mathbb{Z}/(l^n))$  such that  $a(\rho) = 0$  using the notation of Lemma 8.6. Then  $\rho$  is unramified hence it represents the unique element of  $\text{Def}_{\min}(\mathbb{Z}/(l^n)[\epsilon])$  which corresponds to the zero element of  $\text{Adm}(\mathbb{Z}/(l^n))$ . The claim now follows from Proposition 8.7.  $\square$

**Corollary 8.9.** *The Eisenstein ideal  $\mathfrak{E}(\mathfrak{p})$  is locally principal.*

**Proof.** Note that the maximal ideal of the local ring  $R(\mathfrak{p})$  is  $(I_R, l)$ . According to Propositions 8.8 the  $\mathbb{F}_l$ -dimension of the reduced tangent space  $(I_R, l)/(I_R^2, l)$  is at most one hence  $R(\mathfrak{p})$  is generated by a single element over  $\mathbb{Z}_l$ . Because  $T(\mathfrak{p})$  is a quotient of  $R(\mathfrak{p})$  by Proposition 7.8 the latter is also generated by a single element over  $\mathbb{Z}_l$ .  $\square$

**Definition 8.10.** Let us forget for a moment the notation introduced in chapter seven and let  $\mathcal{O}$  be a complete discrete valuation ring with residue field  $\mathbf{k}$ . Suppose that we have a commutative diagram of surjective homomorphism of complete Noetherian local  $\mathcal{O}$ -algebras:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & T \\ & \searrow \pi_R & \swarrow \pi_T \\ & \mathcal{O} & \end{array}$$

Assume that  $T$  is finitely generated and free as an  $\mathcal{O}$ -module. Let  $I_R$  and  $I_T$  denote the kernel of the homomorphism  $\pi_R$  and  $\pi_T$ , respectively. The congruence ideal  $\eta_T$  of  $T$  is defined to be the image  $\pi_T(\text{Ann}_T(I_T))$  of the annihilator of the ideal  $I_T$  in the algebra  $T$ . For every finitely generated and torsion  $\mathcal{O}$ -module  $M$  let  $\text{length}_{\mathcal{O}}(M)$  denote the number of Jordan-Hölder components of  $M$ .

**Theorem (Wiles-Lenstra) 8.11.** *Suppose that  $\eta_T \neq 0$ . Then*

$$\text{length}_{\mathcal{O}}(I_R/I_R^2) \leq \text{length}_{\mathcal{O}}(\mathcal{O}/\eta_T)$$

*and equality holds if and only if  $\phi$  is an isomorphism between complete intersections over  $\mathcal{O}$ .*

**Proof.** This is Criterion I of [3] on page 343.  $\square$

**Theorem 8.12.** *The  $\mathbb{Z}_l$ -homomorphism  $\phi : R(\mathfrak{p}) \rightarrow T(\mathfrak{p})$  is an isomorphism.*

Note that this result with Proposition 8.8 and Theorem 4.5 implies Theorem 1.2.

**Proof.** We wish to use Theorem 8.11 when  $\mathcal{O} = \mathbb{Z}_l$ ,  $R = R(\mathfrak{p})$ ,  $T = T(\mathfrak{p})$  and  $\phi$  is the homomorphism constructed in the proof of Proposition 7.8. Let  $\pi_R$  denote the homomorphism defined in Definition 7.4: in this case  $I_R$  is the ideal introduced in Definition 7.4. Let  $I_T$  denote the ideal generated by the image of  $\widehat{\mathfrak{E}}(\mathfrak{p})$  with respect to the projection  $\widehat{\mathbb{T}}(\mathfrak{p}) \rightarrow T(\mathfrak{p})$ . As we saw in the proof of Proposition 7.8 we have  $\mathbb{Z}_l = T(\mathfrak{p})/I_T$  and the factorization map  $\pi_T : T(\mathfrak{p}) \rightarrow T(\mathfrak{p})/I_T$  makes the diagram in Definition 8.10 commutative. Let  $T_0(\mathfrak{p})$  denote the completion of  $\mathbb{T}(\mathfrak{p})$  with respect to the maximal ideal  $(l, \mathfrak{E}(\mathfrak{p}))$  and let  $\pi_0 : T(\mathfrak{p}) \rightarrow T_0(\mathfrak{p})$  denote the surjection induced by the  $\widehat{\mathbb{T}}(\mathfrak{p}) \rightarrow \mathbb{T}(\mathfrak{p})$ . The direct sum  $\pi_0 \oplus \pi_T : T(\mathfrak{p}) \rightarrow T_0(\mathfrak{p}) \oplus \mathbb{Z}_l$  is injective and  $\text{Ann}_{T(\mathfrak{p})}(I_T)$  is equal to the part of  $(\pi_0 \oplus \pi_T)(T(\mathfrak{p}))$  lying in the second factor  $\mathbb{Z}_l$ . If  $0 \oplus n \in \text{Ann}_{T(\mathfrak{p})}(I_T)$  then  $n \oplus 0 \in (\pi_0 \oplus \pi_T)(T(\mathfrak{p}))$ . The part of  $\pi_0 \oplus \pi_T(T(\mathfrak{p}))$  lying in the first factor  $T_0(\mathfrak{p})$  is the ideal generated by the image of  $\mathfrak{E}(\mathfrak{p})$  with respect to the canonical map  $\mathbb{T}(\mathfrak{p}) \rightarrow T_0(\mathfrak{p})$ . According to claim (vi) of Proposition 7.11 of [19] on pages 180-181 the cyclic group  $\mathbb{T}_l(\mathfrak{p})/\mathfrak{E}_l(\mathfrak{p})$  is finite and its order is divisible by  $l(\mathfrak{p})$ . Hence  $n\mathbb{Z}_l \subseteq l(\mathfrak{q})\mathbb{Z}_l$  for every  $n$  as above and the criterion of Wiles-Lenstra is satisfied by Proposition 8.8.  $\square$

## 9. DIOPHANTINE APPLICATIONS

**Definition 9.1.** The deformation theoretical methods of this paper also give an alternative route to prove the main diophantine results of the paper [19]. The most important advantage of this method is that we do not need the analysis of the special fiber of the modular curves  $X_0(\mathfrak{p})$  and  $X_1(\mathfrak{p})$  at the prime  $\mathfrak{p}$  which occupies chapter 8 of the paper quoted above. In the rest of this paper we give a short description of this alternative route. We will repeat some of the arguments presented in [19] for the sake of exposition. Let  $\mathcal{E}(\mathfrak{p})$  denote the largest torsion subgroup of  $J_0(\mathfrak{p})(\overline{F})$  annihilated by the Eisenstein ideal  $\mathfrak{E}(\mathfrak{p}) \triangleleft \mathbb{T}(\mathfrak{p})$ . In the proof of the following key proposition the Gorenstein property plays an essential role.

**Proposition 9.2.** *The order of the group  $\mathcal{E}(\mathfrak{p})$  divides  $N(\mathfrak{p})^2$ .*

**Proof.** For every group  $G$  and prime number  $l$  let  $G_l$  denote its maximal  $l$ -primary subgroup. It is sufficient to prove that  $\mathcal{E}(\mathfrak{p})_l$  divides  $l(\mathfrak{p})^2$  for every prime number  $l$  where  $l(\mathfrak{p})$  denote the largest power of  $l$  dividing  $N(\mathfrak{p})$ . By Theorem 1.4 we may assume that  $l \neq p$ . Let  $\mu_\infty \subset \mathbb{C}_\infty^*$  denote the subgroup of the roots of unity as in the proof of Lemma 5.9. The Pontryagin dual  $P_l$  of the  $l$ -primary torsion  $Q_l$  of the group  $\text{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mu_\infty)$  is the  $\mathbb{Z}_l$ -dual of a locally free  $\mathbb{T}_l(\mathfrak{p})$ -module of rank one by claim (v) of Proposition 7.11 of [19] on pages 160-161. In particular the part of  $Q_l$  annihilated by the Eisenstein ideal has order  $l(\mathfrak{p})$  by the Gorenstein property. On the other hand the Pontryagin dual of the  $l$ -primary torsion  $R_l$  of the quotient of the torsion group of  $J_0(\mathfrak{p})(\mathbb{C}_\infty)$  by the image of  $\text{Hom}(\overline{\Gamma}_0(\mathfrak{p}), \mu_\infty)$  with respect to the map  $\Psi_{AJ}$  is the  $\mathbb{Z}_l$ -dual of  $P_l$ . Hence the part of  $R_l$  annihilated by the Eisenstein ideal has order  $l(\mathfrak{p})$ , too. Therefore  $\mathcal{E}(\mathfrak{p})_l$  has a two-step filtration such that the orders of the steps divide  $l(\mathfrak{p})$ .  $\square$

Let  $\mathcal{C}(\mathfrak{p}) \subset J_0(\mathfrak{p})(\overline{F})$  and  $\mathcal{S}(\mathfrak{p}) \subset J_0(\mathfrak{p})(\overline{F})$  denote the cuspidal divisor group and the Shimura group, respectively. (For definition see Definition 1.3 and Definition

1.5 of [19] on page 132, respectively.) The group  $\mathcal{C}(\mathfrak{p})$  lies in  $J_0(\mathfrak{p})(F)$  while the group  $\mathcal{S}(\mathfrak{p})$  is  $\mu$ -type. Let  $t(\mathfrak{p})$  denote the greatest common divisor of  $N(\mathfrak{p})$  and  $q - 1$ . We will need the following facts:

**Proposition 9.3.** *The following holds:*

- (i) *the groups  $\mathcal{C}(\mathfrak{p})$  and  $\mathcal{S}(\mathfrak{p})$  are cyclic of order  $N(\mathfrak{p})$ ,*
- (ii) *the intersection of  $\mathcal{C}(\mathfrak{p})$  and  $\mathcal{S}(\mathfrak{p})$  is their unique cyclic group of order  $t(\mathfrak{p})$ .*

**Proof.** Claim (i) is just Corollary 5.11 of [7] on page 235 and Lemma 8.17 of [19] on page 171. For the proof of claim (ii) see Proposition 9.3 of [19] on pages 175-176.  $\square$

In the paper [19] we also introduced another group  $\mathcal{D}(\mathfrak{p})[l] \subset J_0(\mathfrak{p})(\overline{F})$  for every prime number  $l$  dividing  $t(\mathfrak{p})$ . (For definition see Definitions 9.4 and 9.17 on pages 176 and 183 of [19], respectively.) The group  $\mathcal{D}(\mathfrak{p})[l]$  is  $l$ -torsion and contains the  $l$ -torsion subgroup  $\mathcal{S}(\mathfrak{p})[l]$  of the Shimura group  $\mathcal{S}(\mathfrak{p})$ . Let  $\mathcal{F}(\mathfrak{p})[l]$  denote the quotient of  $\mathcal{D}(\mathfrak{p})[l]$  by its subgroup  $\mathcal{S}(\mathfrak{p})[l]$ .

**Proposition 9.4.** *The following holds:*

- (i) *the Galois modules  $\mathcal{S}(\mathfrak{p})[l]$  and  $\mathcal{F}(\mathfrak{p})[l]$  are constant of order  $l$ ,*
- (ii) *the Galois module  $\mathcal{D}(\mathfrak{p})[l]$  is everywhere unramified,*
- (iii) *the Galois module  $\mathcal{D}(\mathfrak{p})[l]$  is contained in  $\mathcal{E}(\mathfrak{p})$ ,*
- (iv) *the exact sequence:*

$$0 \rightarrow \mathcal{S}(\mathfrak{p})[l] \rightarrow \mathcal{D}(\mathfrak{p})[l] \rightarrow \mathcal{F}(\mathfrak{p})[l] \rightarrow 0$$

*of Galois modules does not split over  $F$ .*

**Proof.** This is just Proposition 9.18 of [19] on pages 184-185.  $\square$

Let  $\mathcal{T}(\mathfrak{p}) \subset J_0(\mathfrak{p})(\overline{F})$  and  $\mathcal{M}(\mathfrak{p}) \subset J_0(\mathfrak{p})(\overline{F})$  denote the torsion subgroup of  $J_0(\mathfrak{p})(F)$  and the maximal  $\mu$ -type étale subgroup scheme of  $J_0(\mathfrak{p})$ , respectively. The following lemma is an easy consequence of the fact that neither  $\mathcal{T}(\mathfrak{p})$  nor  $\mathcal{M}(\mathfrak{p})$  has  $p$ -torsion and the Eichler-Shimura relations.

**Lemma 9.5.** *The groups  $\mathcal{T}(\mathfrak{p})$  and  $\mathcal{M}(\mathfrak{p})$  are contained by  $\mathcal{E}(\mathfrak{p})$ .*

**Proof.** For proof see Lemma 7.16 on page 163 and Lemma 10.4 on pages 186-187 of the paper [19].  $\square$

The main diophantine result of [19] is:

**Theorem 9.6.** *We have  $\mathcal{T}(\mathfrak{p}) = \mathcal{C}(\mathfrak{p})$  and  $\mathcal{M}(\mathfrak{p}) = \mathcal{S}(\mathfrak{p})$ .*

**Proof.** We are going to show the equalities  $\mathcal{T}(\mathfrak{p})_l = \mathcal{C}(\mathfrak{p})_l$  and  $\mathcal{M}(\mathfrak{p})_l = \mathcal{S}(\mathfrak{p})_l$  for every prime number  $l$ . We may assume that  $l$  is Eisenstein that is  $l$  divides  $N(\mathfrak{p})$ . First assume that  $l$  is a prime number which does not divide  $q - 1$ . In this case the intersection of the groups  $\mathcal{C}(\mathfrak{p})_l$  and  $\mathcal{S}(\mathfrak{p})_l$  is trivial because the action of the absolute Galois group of  $F$  does not fix any non-zero element of an  $l$ -primary  $\mu$ -type Galois module. On the other hand the order of these groups is  $l(\mathfrak{p})$  by claim (i) of Proposition 9.3 hence their direct sum has the same order as  $\mathcal{E}(\mathfrak{p})_l$  by Proposition 9.2. Therefore  $\mathcal{E}(\mathfrak{p})_l$  and the direct sum of  $\mathcal{C}(\mathfrak{p})_l$  and  $\mathcal{S}(\mathfrak{p})_l$  are equal. Hence  $\mathcal{C}(\mathfrak{p})_l$  and  $\mathcal{S}(\mathfrak{p})_l$  is the maximal constant and  $\mu$ -type Galois module of  $\mathcal{E}(\mathfrak{p})_l$ , respectively. So  $\mathcal{T}(\mathfrak{p})_l = \mathcal{C}(\mathfrak{p})_l$  and  $\mathcal{M}(\mathfrak{p})_l = \mathcal{S}(\mathfrak{p})_l$  by Lemma 9.5.

Assume now that  $l$  is a prime number which does divide  $q - 1$ . Then it also divides  $t(\mathfrak{p})$  because it is Eisenstein. By claim (iii) of Proposition 9.4 the group  $\mathcal{E}(\mathfrak{p})[l]$  contains  $\mathcal{D}(\mathfrak{p})[l]$ . We saw in the proof of Proposition 9.2 that  $\mathcal{E}(\mathfrak{p})_l$  has a two-step filtration such that the steps are cyclic groups. Hence the orders of  $\mathcal{E}(\mathfrak{p})[l]$  and  $\mathcal{D}(\mathfrak{p})[l]$  are equal by claim (i) of Proposition 9.4 so the groups  $\mathcal{E}(\mathfrak{p})[l]$  and  $\mathcal{D}(\mathfrak{p})[l]$  must be equal, too. Now we are going to prove that  $\mathcal{T}(\mathfrak{p})_l = \mathcal{C}(\mathfrak{p})_l$  and  $\mathcal{M}(\mathfrak{p})_l = \mathcal{S}(\mathfrak{p})_l$ . If this claim is false then there is an element  $x$  in  $\mathcal{M}(\mathfrak{p})_l - \mathcal{S}(\mathfrak{p})_l$  (resp. in  $\mathcal{T}(\mathfrak{p})_l - \mathcal{C}(\mathfrak{p})_l$ ) such that  $lx$  is in  $\mathcal{S}(\mathfrak{p})_l$  (resp. in  $\mathcal{C}(\mathfrak{p})_l$ ). The element  $x$  is annihilated by  $l(\mathfrak{p})$ , since it is annihilated by the Eisenstein ideal. Therefore  $lx$  is annihilated by  $\frac{l(\mathfrak{p})}{l}$ . Since both  $\mathcal{S}(\mathfrak{p})_l$  and  $\mathcal{C}(\mathfrak{p})_l$  are cyclic of order  $l(\mathfrak{p})$ , the element  $lx$  must have an  $l$ -th root  $u$  in  $\mathcal{S}(\mathfrak{p})_l$  (resp. in  $\mathcal{C}(\mathfrak{p})_l$ ) by the above. Subtracting  $u$  from  $x$  we get that we may assume that  $x$  is  $l$ -torsion. Hence we must have  $x \in \mathcal{D}(\mathfrak{p})[l]$  by the above. Since  $\mathcal{S}(\mathfrak{p})[l]$  is the maximal constant as well as  $\mu$ -type subgroup of  $\mathcal{D}(\mathfrak{p})[l]$  by claims (ii) and (iv) of Proposition 9.4 we conclude that  $x$  is actually in  $\mathcal{S}(\mathfrak{p})[l]$ . The intersection of  $\mathcal{S}(\mathfrak{p})_l$  and  $\mathcal{C}(\mathfrak{p})_l$  is exactly the largest constant Galois submodule of the former by claim (ii) of Proposition 9.3, so the claim is now clear.  $\square$

## REFERENCES

1. F. Calegari and M. Emerton, *On the ramification of Hecke algebras at Eisenstein primes*, Invent. Math. **160** (2005), 97–144.
2. B. De Smit and H. W. Lenstra, *Explicit construction of universal deformation rings*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer-Verlag, Berlin-Heidelberg-New York, 1997, pp. 313–326.
3. B. De Smit, K. Rubin and R. Schoof, *Criteria for complete intersections*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer-Verlag, Berlin-Heidelberg-New York, 1997, pp. 343–356.
4. V. G. Drinfeld, *Elliptic modules*, [translation], Mat. Sbornik **23** (1974), 561–592.
5. E.-U. Gekeler, *Zur Arithmetik von Drinfeld-Monduln*, Math. Ann. **262** (1983), 167–182.
6. E.-U. Gekeler, *Drinfeld modular curves*, L.N.M. 1231, Springer, Berlin-Heidelberg-New York, 1986.
7. E.-U. Gekeler, *Über Drinfeld'sche Modulkurven von Hecke-Typ*, Comp. Math. **57** (1986), 219–236.
8. E.-U. Gekeler, *On the cuspidal divisor class group of a Drinfeld modular curve*, Doc. Math. **2** (1997), 351–374.
9. E.-U. Gekeler, *On the Drinfeld discriminant function*, Comp. Math. **106** (1997), 181–202.
10. E.-U. Gekeler, *Cuspidal divisor class groups of modular curves*, Algebraic number theory and Diophantine analysis (Graz, 1998), de Gruyter, Berlin, 2000, pp. 163–189.
11. E.-U. Gekeler and U. Nonnengardt, *Fundamental domains of some arithmetic groups over function fields*, Int. J. Math. **6** (1995), 689–708.
12. E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. reine angew. Math. **476** (1996), 27–93.
13. A. Grothendieck, *Revêtements étales et group fondamental*, (SGA1, 1960–61), Lecture Notes in Mathematics, 224, Springer-Verlag, Berlin-Heidelberg-New York, 1971.
14. H. Jacquet and R.P. Langlands, *Automorphic forms on  $GL(2)$* , Springer, Berlin-Heidelberg-New York, 1970.
15. N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton, 1985.
16. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.
17. B. Mazur, *Deforming Galois representations*, Galois groups over  $\mathbb{Q}$  (Ihara, Ribet, Serre, eds.), MSRI Publications, Springer-Verlag, 1989, pp. 385–437.
18. J. S. Milne, *Étale cohomology*, Princeton University Press, Princeton, 1980.

19. A. Pál, *On the torsion of the Mordell-Weil group of the Jacobian of Drinfeld modular curves*, Documenta Math **10** (2005), 131–198.
20. J.-P. Serre, *Arbres, amalgames,  $SL_2$* , Société Mathématique de France, Paris, 1977.
21. M. Schlessinger, *Functors on Artin rings*, Trans. A.M.S. **130** (1968), 208–222.
22. A. Tamagawa, *The Eisenstein quotient of the Jacobian variety of a Drinfeld modular curve*, Publ. Res. Inst. Math. Sci. **31** (1995), 203–246.
23. J. Teitelbaum, *Modular symbols for  $\mathbb{F}_q(T)$* , Duke Math. **68** (1992), 271–295.
24. A. Weil, *Dirichlet series and automorphic forms*, Springer, Berlin-Heidelberg-New York, 1971.